



# La projection d'usage des TICs : la composition de fictions axiomatiques au service de la recherche technologique

Emmanuel Anjembe

## ► To cite this version:

Emmanuel Anjembe. La projection d'usage des TICs : la composition de fictions axiomatiques au service de la recherche technologique. Sociologie. Université de Grenoble, 2014. Français. NNT : 2014GRENH014 . tel-01161215

**HAL Id: tel-01161215**

**<https://theses.hal.science/tel-01161215>**

Submitted on 8 Jun 2015

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

## THÈSE

Pour obtenir le grade de

## DOCTEUR DE L'UNIVERSITÉ DE GRENOBLE

Spécialité : **Science Politique**

Arrêté ministériel : 7 août 2006

Présentée par

**Emmanuel ANJEMBE**

Thèse dirigée par **Bernard DENNI** et  
codirigée par **Céline VERCHERE**

préparée au sein du **Laboratoire PACTE/CNRS**  
dans l'**École Doctorale "Sciences de l'Homme, du Politique et  
du Territoire (ED SHPT n°454)**

## La projection d'usage des TICs

### La composition de fictions axiomatiques au service de la recherche technologique

Thèse soutenue publiquement le « **20 octobre 2014** »,  
devant le jury composé de :

**M. Dominique VINCK**

Professeur d'Université, Uni. de Lausanne, Président

**Mme Josiane JOUET**

Professeure d'Université, Université Paris 2, Rapporteure

**Mme Joëlle LE MAREC**

Professeure d'Université, Université Paris 7, Rapporteure

**M., Bernard DENNI**

Professeur d'Université, Directeur de thèse

**Mme Céline VERCHERE**

Docteure, CEA Grenoble



*« Oui, la nuit est venue, un autre monde se lève.  
Dur, cynique, analphabète, amnésique,  
tournant sans raison...  
Etalé, mis à plat,  
comme si on avait supprimé  
la perspective ,le point de fuite... et  
le plus étrange, c'est que les morts-vivants  
de ce monde sont construits sur le monde d'avant...  
Leurs réflexes, leurs sensations, leur tête sont d'avant... »*

*22, Sollers, Femmes, 1983*

# Remerciements



Le recours à la métaphore de la course de fond pour saisir le travail de thèse est d'un clacissisme attendu : on fait coller les premières foulées aux premières lignes enthousiastes et on assimile la dernière ligne droite aux lâchés d'encre conclusifs. Tout porte le thésard à s'y décrire sous les traits d'un marathonien, habilement dépouillé de tapageuses épithètes homériques, mais discrètement paré de l'étoffe des héros. En se retraçant tourneboulant tout du long de son parcours, il convoque des oxymores d'expériences qui fondent la turbulence de l'épreuve : les solitudes des coureurs de fond et les encouragements des publics amateurs, les soirées brumeuses et les faux soleils matinaux, les crampes espiègles et les fulgurantes détentes, les troubles carentiels et les trop-pleins nourrissant, la souffrance juste et la douleur maligne. La métaphore est rarement filée jusqu'à épuisement mais sa puissance d'évocation maintient l'ellipse efficace.

Les lignes qui suivent participent du même laconisme maladroit. Elles sont un concentré d'éléments hétéroclites et de phénomènes contradictoires. Elles disent à la fois la gratitude et l'égoïsme, la bienveillance des dons et la nécessité des contre-dons. Parce qu'elles disent mille rhizomes polymorphes, on s'excusera de s'y constituer barycentre du réseau. L'opération vise à remercier ceux qui m'ont accompagné dans l'épreuve en dégageant du bout de chaque rue les montagnes de doutes, de suffisance, d'absurdité ou de vides qui ont pu se dresser sur un chemin qu'ils ont fait leur. Il ne faut cependant pas coller à chaque ligne une foulée différente mais croiser dans cet inventaire l'œil engourdi d'un coureur familial qui, à la fin de sa course solitaire, dit le fond d'une reconnaissance confidentielle et sincère. Une reconnaissance qu'il espère partagée.

- Bernard Denni, directeur de cette thèse, et Céline Verchère, encadrante de cette thèse.
- Miguel Aubouy, Tiana Delhome, Timothée Jobert du CEA-LETI et Nicolas Schunadel et Julien Soler
- Magali Cros, Michel Ida et Philippe Mallein du Minatec Ideas Laboratory
- Valérie Chanal, Fabrice Forest, Olivier Lavoisy de Umanlab
- Les équipes de projets COPRIM et IAM
- Igor Babou, Clémence Emprun, Joëlle le Marec, Jérôme Michalon et Ludivine Raimondo du Cluster 14
- Mathieu Brugidou et Arthur Jobert d'EdF

- Pascal Trompette et Dominique Vinck de PACTE ainsi que toute l'équipe administrative
- Valérie Perret de l'UPMF
- Daniel Guiraud, maire des Lilas
- Cléa Caulcutt, Aisling Corcoran et Emmanuel Madibane for translations
- Les familles Askari, Bellal, Boschetti, Bellevilloise, Beaurepaixoise, Bonnet, Brener, Canales, Caulcutt, Demaison, De Metz, Delors, Gourgues, Hamzaoui, Madibane, Mallein, Munyikwa, Pierot-Théry, Puissant, Roumet, Roux, Sanchez, Vallée, Vallet.
- Sarah B.
- Ma mère et Ma famille.

# Table des matières

<b>Table des matières.....</b>	<b>6</b>
<b>Introduction.....</b>	<b>9</b>
<b>Partie 1. L'usage, carrières d'un concept.....</b>	<b>35</b>
<b>I - L'usage, objet d'une pratique poïétique.....</b>	<b>46</b>
A - Le passage à l'acte déviant : l'usage, de la statistique au construit social .....	47
B - L'apprentissage social : l'établissement d'un collège invisible .....	53
C - La désignation publique : la production scientifique comme lieu d'organisation.....	56
D - La perpétuation de pratiques et savoir-faire : l'espace national comme ancrage.....	58
<b>II - L'usage, objet d'une pratique pythique.....</b>	<b>62</b>
A - Le passage à l'acte déviant : le pas tournant de la méthode CAUTIC™ .....	64
B - L'apprentissage social : Philippe Mallein, point de ralliement d'une science entrepreneuriale .....	71
C - La désignation publique : CAUTIC™, une méthode d'intervention engagée .....	73
D - La perpétuation de pratiques et savoir-faire : l'émergence locale d'une relève.....	78
<b>III - La projection d'usage, objet d'une pratique sibylline .....</b>	<b>81</b>
A - Le passage à l'acte déviant : des conséquences d'avoir pour dessein l'innovation technologique.....	82
B - L'apprentissage social : la prise du tournant expérientiel .....	92
C - La désignation publique : le poids des organisations industrielles dans la structuration de la pratique .....	98
D - La perpétuation de pratiques et savoir-faire : la fragmentation des espaces d'expression.....	100
<b>IV - Conclusion de la partie I .....</b>	<b>103</b>
<b>Partie 2. La projection d'usage, genèse d'une écologie socio-technique .....</b>	<b>106</b>
<b>V - Le projection d'une écologie socio-technique stable .....</b>	<b>110</b>
A - Positionner le projet dans un cadre de fonctionnement circonscrit.....	111
B - Positionner le projet dans un cadre d'usage projeté .....	115
C - Consolider la projection d'une écologie socio-technique.....	118
<b>VI - La scénarisation comme modalité de projection.....</b>	<b>123</b>
<b>VII - L'observation participante comme méthode d'investigation.....</b>	<b>131</b>
A - L'OP comme moyen de suivre les acteurs/actants .....	131
B - Observer (quasi) clandestinement une organisation formelle : la participation totale au projet COPRIM.....	137
C - Questions de distance réflexive au terrain.....	143
<b>VIII - Conclusion de la partie II.....</b>	<b>150</b>
<b>Partie 3. Le scénario, investissement de forme fictionnelle .....</b>	<b>152</b>
<b>IX - Le scénario, acte de langage.....</b>	<b>156</b>
A - Le scénario, un acte de langage scientifique .....	158
B - Le scénario, un acte de langage situé .....	162

C - Le scénario, un acte de langage prévisible .....	163
D - Le scénario, un acte de langage social .....	174
<b>X - Le scénario : acte de croyance.....</b>	<b>181</b>
A - Le projet, réseau local relais de l'enthousiasme technologique .....	187
B - La sécurité au cœur de l'intrigue technologique .....	191
<b>XI - Conclusion de la partie III .....</b>	<b>227</b>
<b><i>Partie 4. La scénarisation ou la composition d'axiomes.....</i></b>	<b><i>229</i></b>
<b>XII - La scénarisation : co-conception d'une « infrastructure-frontière » .....</b>	<b>232</b>
A - Le scénario : une infrastructure frontière ultra-locale reposant sur une écologie d'objets aux statuts fluctuants.....	232
B - La naturalisation de l'infrastructure-frontière .....	243
<b>XIII - La scénarisation : articuler et catégoriser les déplacements .....</b>	<b>257</b>
A - Le travail d'articulation : la distribution de l'expertise entre les strates .....	258
B - Le travail de catégorisation : la convergence de choses .....	263
C - La composition d'axiomes.....	275
<b>XIV - Conclusion de la partie IV.....</b>	<b>282</b>
<b><i>Conclusion générale .....</i></b>	<b><i>285</i></b>
<b><i>Bibliographie.....</i></b>	<b><i>290</i></b>
<b><i>Annexes .....</i></b>	<b><i>307</i></b>
<b><i>Annexe 1. Objets mobilisés durant la conception du scénario.....</i></b>	<b><i>308</i></b>
<b><i>Annexe 2. State of the art NFC and Privacy.....</i></b>	<b><i>332</i></b>
<b><i>Annexe 3. COPRIM Scenarios. Specifications.....</i></b>	<b><i>437</i></b>
<b><i>Annexe 4. Technical Annex.....</i></b>	<b><i>477</i></b>
<b><i>Annexe 5. Les trois temps du travail de scénarisation.....</i></b>	<b><i>526</i></b>
A - La stabilisation de l'intrigue : le problème technologique comme consensus .....	529
B - La stabilisation de l'instanciation .....	540
C - L'émergence de champs du possible .....	546

# Introduction

« Hippogriffe impétueux, qui luttas de vitesse avec le vent,  
éclaire sans flammes, oiseau sans plumes colorées,  
poisson sans écailles, quadrupède sans instinct naturel,  
pourquoi t'élancer, t'emporter, te précipiter  
dans le confus labyrinthe de ces roches dépouillées ?  
Arrête-toi sur cette montagne,  
où les bêtes pourraient bien aussi avoir leur Phaéton. »

*Calderon (1996). La vie est un songe, Paris, Le livre de poche, p.7*

Alors que la crise financière amorcée à l'été 2007 produit encore des effets dévastateurs sur l'équilibre et le dynamisme économique mondial, l'année 2009, sous l'impulsion de la présidence française du conseil de l'Union Européenne (juillet-décembre 2008), a été proclamée « année de la créativité et de l'innovation » par la Commission Européenne. Les ambitions de cette initiative<sup>1</sup> sont les suivantes :

- « créer un environnement propice à l'innovation ;
- démontrer l'importance de la créativité, de l'innovation et de l'esprit d'entreprise, notamment en ce qui concerne la croissance économique et l'emploi ;
- promouvoir l'acquisition de compétences essentielles dans des contextes professionnels et sociaux ;
- promouvoir le rôle du secteur de la conception ;
- encourager la créativité et l'innovation dans les organisations publiques et privées. »

Cette inscription de l'innovation et de la créativité à l'agenda des politiques communautaires participe d'un mouvement plus large d'adhésion des acteurs majeurs des centres de décisions politiques et économiques au crédo de l'innovation technologique comme moteur de croissance et de développement. L'Organisation de Coopération et de Développement Economiques (OCDE) affirme ainsi :

*« L'innovation est un facteur déterminant de la croissance et des performances de l'économie mondialisée. Elle donne naissance à de nouvelles technologies et de nouveaux produits qui aident à répondre aux enjeux mondiaux comme ceux de la santé ou de l'environnement. En transformant les modalités de production des biens et de prestation des services, elle stimule la productivité, crée des emplois et contribue à améliorer la qualité de vie des citoyens. »* (OCDE, 2007 p. 44)

Sur un plan analytique, cette foi dans les vertus de l'innovation technologique est symptomatique de l'entrée dans une période de « modernité tardive » agie par la quête de nouveauté et de destruction créatrice schumpetérienne (Boutinet, 2007 p. 322-323) :

*« A la suite des travaux de Schumpeter (1912), nous pouvons mieux mesurer en quoi nos cultures industrielles et postindustrielles nous entraînent de plus en plus vers une recherche obstinée de nouveauté, à travers cette destruction créatrice qui pousse à l'obsolescence pour mieux assurer l'avènement du nouveau. Une telle recherche de*

---

<sup>1</sup> (16 décembre 2008)



*nouveauté prend spécialement deux formes caractéristiques [Flichy, 1995] : l'innovation radicale la plus ancienne et qui a déjà ses lettres de noblesse se manifeste en même temps comme la plus durable, la plus coûteuse et la forme la plus rare ; l'innovation incrémentale, la plus récente, est aussi la plus répandue et la plus éphémère. Seule la première, malgré les problèmes qu'elle peut poser, possède les caractéristiques de l'invention propre au projet créateur à travers la mise en évidence d'un inédit technique ou social. La seconde n'est que la réorganisation de l'existant sous l'une ou l'autre variante qui ne comporte aucune singularité. Parce que le projet d'innovation radicale ne peut surgir qu'à des moments exceptionnels qui impliquent pour se réaliser la conjonction de différentes opportunités, il a été doublé par le projet d'innovation incrémentale ; celui-ci sans avouer son nom cherche néanmoins à faire entrer le changement dans le moindre de nos gestes quotidiens. De ce point de vue, l'innovation incrémentale, plus facile à manipuler, plus séduisante à court terme, exprime bien l'une des tendances fortes de notre modernité tardive, celle d'instaurer un présent vêtu des oripeaux de la nouveauté en opposition avec un passé considéré comme révolu, permettant de bannir les temporalités de la répétition. »*

L'innovation donc, soit l'intégration réussie d'une invention sur le marché, est une préoccupation d'autant plus stratégique que l'environnement économique globalisé est aujourd'hui caractérisé par son « *hypercompétitivité* » (D'Avenir & Gunther, 1994). La pérennité des gains de compétitivité escomptés des innovations est menacée par le rythme de renouvellement de celles-ci ainsi que par la concurrence. L'innovation, bien plus qu'une nécessité, est présentée comme une condition de survie des organisations :

*« En moins d'un demi-siècle, le processus de génération des innovations est devenu le terrain de compétition majeur du capitalisme contemporain et un moyen essentiel du développement durable des sociétés contemporaines. Pour les entreprises [...] il s'agit de survivre dans un capitalisme de l'innovation intensive. Dans une société habituée à renouveler régulièrement ses projets et ses modes de vie, il s'agit même du mode fondamental de création de valeur. »* (Le Masson, Hatchuel & Weil, 2006 p. 23 cité par Gillier 2010)

Ce « *capitalisme d'innovation intensive* » a notamment pour conséquence l'extension des domaines explorés par l'innovation. En effet, tandis que la stimulation des activités de R&D<sup>2</sup> est reconnue comme une contribution majeure dans l'avènement d'innovations

<sup>2</sup> « La recherche et le développement expérimental (R&D) englobent les travaux de création entrepris de façon systématique en vue d'accroître la somme des connaissances, y compris la connaissance de l'homme, de la culture et de la société, ainsi que l'utilisation de cette somme de connaissances pour de nouvelles applications. » (OCDE, 2003 p. 34)

technologiques<sup>3</sup>, la R&D n'en constitue pas le seul facteur. Au terme d'une enquête réalisée pour le compte du Ministère de l'Economie, de l'Industrie et de l'Emploi, Pascal Morand et Delphine Manceau (2009) relèvent que pour les entreprises et dirigeants français « *l'innovation est le fruit d'un processus global dans lequel la Recherche et Développement n'est qu'un ingrédient parmi d'autres, à intégrer dans une démarche organisationnelle complexe* » (p.13). Les auteurs critiquent ainsi l'hégémonie d'une vision macroéconomique de l'innovation fondée sur la production de brevets et la R&D. Cette vision repose sur l'établissement d'une identité entre invention et innovation, cette dernière réclamant en réalité la mobilisation de ressources diverses telles que le marketing, le design, la créativité, la stratégie d'entreprise, l'organisation, le recrutement et toutes les composantes du management. La complexité du processus d'innovation est aussi accentuée par l'intensité du capitalisme au sein duquel il prend place. Elle encourage les organisations dont la R&D est le cœur de métier à faire converger deux modèles de gestion de l'innovation (Gillier, 2010) : celui où l'innovation est pensée comme résultant des efforts de recherche scientifique et celui où elle est perçue comme la conséquence d'un management des capacités créatives. Cette convergence de manières de penser, de faire et d'agir à laquelle ces organisations sont contraintes illustre la montée du recours aux expertises comme phénomène caractéristique de notre époque et comme équipement fondamental pour ces acteurs (Trépos, 2001).

Ce recours à ces « *systèmes experts* » est caractéristique de la « *modernité avancée* » (Giddens, 1990). Le sociologue britannique refuse de limiter la modernité à l'appétence pour la nouveauté, comme nous l'avons constaté en ce qui concerne la « *modernité tardive* ». Pour Giddens, c'est l'essence réflexive qui caractérise notre modernité :

« *It is often said that modernity is marked by an appetite for the new, but this is not perhaps completely accurate. What is characteristic of modernity is not an embracing of the new for its own sake, but the presumption of wholesale reflexivity – which of course includes reflection upon the nature of reflection itself.* » (Giddens, 1990 p. 39)

Le recours croissant à des champs d'expertises variés va donc de pair avec cette réflexivité tous azimuts. La modernité avancée place, à cet égard, les sciences sociales, et plus spécifiquement la sociologie, au cœur de l'expression de son dynamisme :

« *The reflection of which the social sciences are the formalized version (a specific genre of expert knowledge) is quite fundamental to the reflexivity of modernity as a whole.*

<sup>3</sup> La politique de l'Union Européenne, dite « Stratégie de Lisbonne », a été adoptée en 2000 pour doter l'UE d'une économie forte et hautement compétitive à l'horizon 2010. L'un des objectifs consistait à porter les dépenses en R&D à 3% du PIB de chaque état membre.

*[...] All the social sciences participate in this reflexive relation, although sociology has an especially central place [...] The pivotal position of sociology in the reflexivity of modernity comes from its role as the most generalized type of reflection upon modern social life. »* (Giddens, 1990 p. 40-41)

C'est au croisement de ces deux idées complémentaires de la modernité, « *tardive* » et « *avancée* », entre dynamiques d'innovation et de réflexivité, que se trouve l'objet de notre investigation : les « *recherches spéculatives pour l'innovation*<sup>4</sup> » (Stewart & Claeys, 2009), et plus particulièrement le recours à la sociologie comme forme d'expertise au service de la conception d'innovations technologiques.

L'instrumentalisation des connaissances sociologiques dans le travail de conception technologique s'inscrit dans la dynamique de rapatriement des sciences sociales comme moyen de réduction de l'incertitude pesant sur le succès de l'innovation. En effet, le passage d'un modèle de production/consommation de masse vers une individualisation de l'offre et de la demande a intensifié la nécessité de multiplier les sources et la nature des connaissances sur l'environnement d'accueil de l'invention. Aujourd'hui, le marketing et la prospective constituent ainsi des composantes importantes du processus d'innovation dans le domaine de la conception technologique<sup>5</sup> : les connaissances et l'action sur les marchés existants et les marchés à venir sont des ressources considérées comme déterminantes. Ces deux disciplines sont impliquées afin de mieux discerner les contours sociodémographiques (âge, sexe, genre, niveau de revenus, etc.) des populations et des territoires à cibler pour favoriser la diffusion des innovations. Dans le champ des Technologies de l'Information et de la Communication (TICs), cet intérêt prend un tour particulier. En effet, ces technologies sont fondamentalement intégrées dans la fabrique sociale du quotidien de leurs utilisateurs (Osimo, 2005). Se lancer dans la conception de celles-ci implique d'octroyer à la réflexion sur leurs « usages » une place de choix dans le processus de conception :

*« [Communication technologies] have no function without connection. Once one focuses, then, on the everyday lives of actual and potential users of such technologies and*

---

<sup>4</sup> « Speculative since it's inventive and involves imagining futures different to the present; research, since it involves scientific methods and the exploration of the unknown and the novel; and innovation, since it is directed at informing and stimulating innovation. » James Stewart and Laurence Claeys, 'Problems and Opportunities of Interdisciplinary Work Involving Users in Speculative Research for Innovation of Novel Ict Applications', in Bartolomeo Sapio et al. (eds.), *The Good, The Bad and The Challenging. The user and the future of information and communication technologies* (Copenhagen, 2009).

<sup>5</sup> « It is worth considering the closeness of technology foresight and market research. Foresight is typically thought of as a perception of events that have yet to occur. Another view, used in the world of business strategy, is that Strategic Foresight is the ability to create and maintain a high-quality, coherent and functional forward view, and to use the insights arising in useful organizational ways. [...] Market research on the other hand is an endeavor that collects data about customers, competitors and markets to analyze it to find patterns and trends. The aim of market research is to attain a higher degree of predictability, certainty and understanding of a certain market. In that respect, foresight and research are ways of improving the view of what is to come, i.e. our possible future, albeit in different ways. » (Un & Price, 2007)

*recognizes that their use does not just involve the object (the machine, the handset, the terminal), but is implicated from the very beginning in networks of connections, both in real and in the mediated world, then it is hardly surprising that the social and cultural dimensions of usage emerge as crucial components of the innovation process. » (Osimo, 2005 p. 102)*

Cette importance accordée à l'« usage » et aux « utilisateurs » se fait par l'intégration, en sus du déploiement de méthodes et d'outils propres au marketing ou à la prospective<sup>6</sup>, de problématiques propres aux sciences sociales durant le processus de conception (Sorensen, 2009). Soit celles-ci sont intégrées au sein de l'écologie de production du savoir des ingénieurs et ceux-ci prennent alors en main l'application des théories et méthodes qu'ils se sont appropriées ; soit les sciences sociales sont intégrées au processus de conception par un « *mode d'appropriation transdisciplinaire* » reposant sur la collaboration d'ingénieurs et de personnels formés aux sciences sociales. C'est cette alternative qui retient ici notre intérêt.

Le recours aux sciences sociales comme ressource pour la conception des TICs est historiquement centré sur l'analyse des interactions hommes/machines. Ainsi, dès les années 70, c'est la psychologie cognitive qui a été mobilisée comme ressource pour adapter le fonctionnement des machines aux modèles cognitifs dans la conception de systèmes informatiques (Bannon & Liam, 1992 ; Agre, 1994). Parallèlement, dans les pays scandinaves, c'est une approche critique des modalités de gouvernance des entreprises qui a été à la base du développement d'un courant de recherche visant à associer les employés à la conception de TICs (Greenbaum & Kyng, 1991). L'objectif était de limiter la mainmise du management sur une division du travail considérée comme déqualifiante pour les employés et défavorable à leur montée en compétences. Ceux-ci basculent, avec cette approche dite scandinave, au centre des processus de conception : leurs compétences propres ainsi que leur environnement de travail sont tenus d'être investigués, soit par le biais de l'enquête sinon par l'implication directe des employés durant la conception. Cependant, c'est d'outre-Atlantique que la mobilisation des sciences sociales et le recours à des chercheurs praticiens vont être systématisés. Ainsi, c'est au Xerox Parc que l'anthropologie connaît ses premières heures de gloire industrielle, notamment à travers le succès retentissant du travail

---

<sup>6</sup> « In the conventional field of market research, it remains difficult for to investigate and explore people in a future context because market research is essentially concerned with supporting the current core business and it mainly focuses on growth based on today's or next year's market, rather than a few years in the future. Although many attempts have been made to ask people about their dreams, aspirations, feelings and thoughts in the future, both the method and the outcomes of such an approach remain questionable and debatable. So whereas technological development happens mostly at the fuzzy front of innovation, market research is usually applied in later end phases of innovation. » (Un and Price 2007: 1761)

ethnométhodologique de Lucy Suchman (1987) qui encourage à penser la cognition comme un phénomène social.

Critique sévère de l'appréhension des interactions homme-machine reprenant des schémas cognitifs ignorant les capacités d'adaptation des acteurs aux changements de situations sociotechniques auxquelles ils sont confrontés durant leur travail, ce plaidoyer pour une appréhension sociale et située de la cognition est révélateur de l'émergence d'un champ de recherche, le CSCW (Computer Supported Cooperative Work). Ce courant est dédié à comprendre et à étudier finement les environnements de travail (« *workplaces* ») en se dégageant d'une lecture de ceux-ci réduite à l'étude du face-à-face entre l'homme et la machine (Lave & Wenger, 1991 ; Heath & Luff, 1992 ; Hutchins, 1995 ; Blomberg, Suchman & Trigg, 1996). Ce courant va être enrichi par les réflexions d'une communauté de chercheurs provenant de la sociologie interactionniste du travail qui vont travailler sur le même objet : la conception de TICs et leur adéquation (ou non) à l'environnement de travail. L'observation des interactions au sein des « *workplaces* » oblige à apprécier les contingences inhérentes au déroulement des tâches, le « *travail invisible* » et *ad hoc* d'adaptation des acteurs (Strauss, 1988) ainsi que le dynamisme des formes de connaissances impliquées. La prise en compte du « *travail d'articulation* », qui consiste à maintenir le bon déroulement de l'activité et qui se fait dans l'ombre de ce qui avait été décidé (Gerson & Star, 1986), va jusqu'à gagner le statut de véritable enjeu de la conception des TICs (Schmidt, K. & Bannon, 1992 ; Cardon, 1997). L'ethnographie des lieux de travail s'impose ainsi, dès la fin des années 80, comme condition préalable à la conception des TICs et à la prise en compte du « *travail d'articulation* » (Bloomberg, 1993 ; Shapiro, 1994 ; Button, Graham, 2000)<sup>7</sup>. Aujourd'hui, les sciences sociales occupent une place de choix au sein des grandes entreprises engagées dans le développement de TICs (Stewart & Claeys, 2009). Les départements R&D d'Intel, de Nokia, de Xerox, de Google, de Yahoo, d'Alcatel Lucent, de France Telecom ou encore de EDF intègrent des équipes de sciences sociales à leurs effectifs. Ce constat, s'il ne doit pas faire miroiter une banalisation de l'incorporation des sciences sociales dans les processus de conception<sup>8</sup>, est symptomatique de l'actuelle

<sup>7</sup> Nous avons volontairement omis d'aborder ici le cas français sur lequel nous revenons dans la première partie de la thèse. Cependant, l'on peut ici affirmer qu'en France, l'incorporation de la sociologie à l'activité de conception a pris son essor durant la même période (Jouët, 2000 ; Jaureguiberry, 2008) Cependant, elle participait moins d'une critique des paradigmes cognitivistes fondés sur les schémas mentaux que d'une tradition d'étude et de réflexion pluridisciplinaire sur l'« usage » des TICs. De ce fait, le travail d'intégration de l'« usage » dans les pratiques de conception n'est pas limité à une insertion des TICs dans un milieu professionnel ; c'est plutôt la sphère domestique, et plus particulièrement le « quotidien », qui retient l'attention des chercheurs. Cette sociologie, dont l'arrière-plan politique est analogue à celui de l'« approche scandinave » dans sa critique d'une appréhension des utilisateurs de TICs comme des êtres passifs, dépouillés de leurs compétences, s'est faite pratique de conception sujette à controverses (voir partie I).

<sup>8</sup> « The most common resource used to interpret user requirements is not social science but the personal experience, knowledge and taste of the designing engineers. » (Sorensen, 2009 p. 107)

diffusion des pratiques sociologiques en dehors des sphères académiques (Pirou, 2008). Ce « *tournant praticien* » caractérisé par « *une croissance rapide d'emplois dans les secteurs non académiques (privés et publics), qui requièrent une expertise et des compétences de sociologie appliquée* » (Pirou, 2008 p. 123) est générateur de nouvelles pratiques portées par les « *praticiens de la sociologie* » :

« Par « *praticiens de la sociologie* », il faut entendre les diplômés de haut niveau en sociologie [DEA, DESS, doctorat ou diplôme équivalent en formation continue], qui utilisent les connaissances de sociologie, en dehors de l'université et de la recherche publique (CNRS, INSERM, INRA...). Ces praticiens de la sociologie sont donc rémunérés par une organisation privée ou publique (à l'exception de l'université et des centres de recherche de la fonction publique.) Ils peuvent exercer en tant qu'indépendants. Ils ont un statut de droit privé. » (Pirou, 2006 p. 14)

Cet « *autre métier* » que celui qui s'exerce dans le monde académique (Alter, 1999 p. 99) se rattache aux « *métiers de l'analyse* » comme la finance, l'informatique, le marketing, la gestion des ressources humaines ou encore la logistique. Il s'en distingue notamment du fait que la sociologie n'ait « *pas (encore ?) rompu avec le milieu académique qui l'a fondée* » (Alter, 1999 p. 101). C'est la persistance de ce cordon ombilical qui rend passionnante l'enquête menée par Odile Pirou sur les praticiens de la sociologie (Pirou, 2006). En s'appuyant sur les acquis de la sociologie des professions et la sociologie des organisations, ses investigations ont permis d'explorer les questions de rôle, de légitimité, de représentation et d'identité de ces praticiens. Ceux-ci sont notamment confrontés à une demande sociale marquée par une exigence d'opérationnalisation, par une grande malléabilité et par les risques de déni de légitimité méthodologique notamment face à des cultures « *techniciennes* », « *gestionnaires* » ou « *administratives* ». Cette demande sociale est également caractérisée par la grande hétérogénéité des objectifs assignés : des demandes d'étude et de diagnostic, de conseil-formation et de pilotage, des demandes d'animation-médiation, d'évaluation et de veille, des demandes de résolution de problèmes et de plus en plus, des demandes d'anticipation<sup>9</sup> auxquelles répondent les recherches spéculatives pour l'innovation. Concernant l'étude des pratiques, l'auteure, en s'appuyant sur la sociologie du travail, a réussi à établir des liens entre celles-ci, les compétences des praticiens et leurs effets sur les systèmes et les acteurs. Elle dégage ainsi trois postures d'expertises

---

<sup>9</sup> « Alors que les demandes d'anticipation n'étaient pas apparues comme telles dans les motivations conduisant au recours de sociologues praticiens dans les années 90, elles représentent aujourd'hui 24% des demandes totales. La fonction d'anticipation et d'aide à la décision des sciences sociales dans la définition des politiques est une tendance qui s'amorce. » (Pirou, 2006 p. 168)

correspondant à des combinaisons de positions, de pratiques et d'engagement chez les praticiens. Dans le cas de l'expertise « *mandatée* », où il s'agit de fournir un diagnostic objectif et ponctuel encadré par une relation de service, l'expert est un chargé d'études menant l'enquête. Dans le cas de l'expert « *traitant* », « *l'expertise s'accompagne d'une prise en charge de la situation. Le praticien qui analyse une situation est aussi un professionnel traitant la même situation. La légitimité de l'expertise ne se dissocie pas du savoir pratique de l'expert.* » (Pirou, 2006 p. 128) Les positions de manager (avec la pratique de pilotage) et de consultant-formateur (avec la pratique d'accompagnement) s'y inscrivent. Enfin, dans le cas de l'expert « *instituant* », l'engagement se fait normatif et vise une modification de l'ordre ancien. Ce type d'expertise est l'œuvre du conseiller (avec une pratique de conseil ou de négociation). En sus d'avoir discerné ces différents niveaux d'expertises et d'engagements, Odile Pirou perçoit la montée de la légitimité du diagnostic et en parallèle celle de l'inférence et du principe de véridiction<sup>10</sup>. Ainsi, s'intéresser aux recherches spéculatives pour l'innovation, c'est donc se pencher sur « *une pratique en mouvement, en profonde refondation dans l'entrée dans le nouveau millénaire (depuis 2000)* » (Pirou, 2008) ; une « *modernité avancée* » marquée par l'intensification et la distribution des capacités et initiatives réflexives. Cependant, si ces résultats nous offrent une fine vue d'ensemble des territoires couverts par la sociologie praticienne, leur visée synthétique donne au final plus à voir la variété des profils des praticiens que leurs pratiques concrètes. Sont ainsi laissées dans l'angle mort les spécificités des terrains au sein desquels les pratiques se déploient, spécificités qui ont éveillé notre intérêt. En effet, ces recherches spéculatives se fabriquent à la genèse des processus de conception, en un lieu qu'il est désormais convenu de nommer le « Fuzzy Front End<sup>11</sup> » de l'innovation (Smith & Reinertsen, 1995 ; Khurana & Rosenthal, 1998 ; Koen et al., 2001 ; Reid & de Brentani, 2004). Antérieur à la phase de développement de l'innovation, ce lieu est marqué par une grande incertitude en termes de nature du travail à effectuer, de financement, d'attentes, en termes de génération de revenus, de date de mise sur le marché du produit conçu et de modalités d'évaluation de la technologie (voir

Tableau 1).

La finalité est ici la production et la consolidation d'un concept à développer dans les phases suivantes du processus de R&D. Ces concepts participent des entreprises de

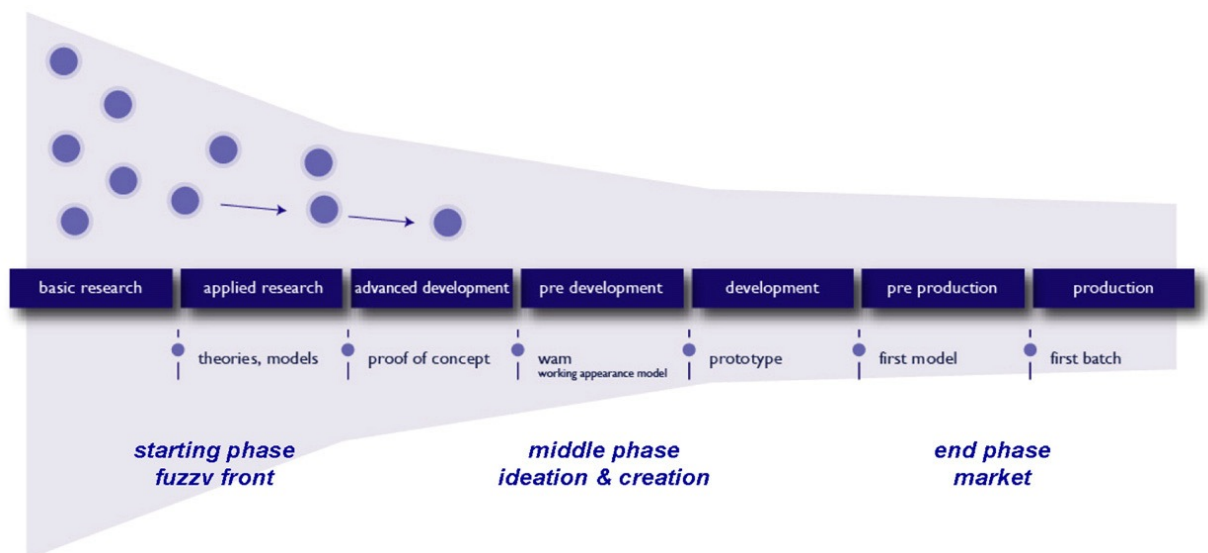
<sup>10</sup> L'inférence fait appel à la capacité des sociologues praticiens à « traduire par des actions et des décisions concrètes le diagnostic (l'analyse) qu'ils ont réalisé. Aujourd'hui, le sociologue est interpellé sur sa capacité à assurer, si ce n'est la réussite, du moins l'opérationnalité de son analyse » (Pirou, 2008 p. 126). En termes de véridiction, en s'inspirant de Foucault, Pirou constate l'injonction faite aux praticiens de produire des connaissances vérifiables ou falsifiables.

<sup>11</sup> L'expression, difficile à traduire, pourrait signifier le front brumeux de l'innovation.

productions de « *perspectives*<sup>12</sup> » (Borup, Brown, Konrad & Lente, 2006). Celles-ci servent de point d'appui à la conception dont elles structurent l'activité, sont pourvoyeuses de légitimité, provoquent l'intérêt et motivent l'investissement. Elles définissent les rôles, clarifient les tâches à effectuer et aident au pilotage et à l'évaluation de l'activité de développement<sup>13</sup>. Ces projections performatives se révèlent, en somme, indispensables au management de l'innovation technologique<sup>14</sup>. Quelles que soient leurs formes, elles constituent un « *point de passage obligatoire* » de l'entreprise de conception (Callon, 1986) :

*«These kinds of dynamics have a particularly salient role to play in the most early stages of technoscientific constructions and innovations. Here it is likely that roles will be ambiguous, lacking form or agreement; regulatory aspects like those of standards and quality control are unlikely to have been developed; market players will experience acute levels of uncertainty in judging appropriate levels of investment; it will probably be the case that numerous competing innovation futures are also being promoted; contestation and conflict may be very high, etc. »* (Borup, Brown, Konrad & Lente, 2006 p. 289)

Figure 1. Les différentes étapes de l'innovation<sup>15</sup> (Un & Price, 2007)



<sup>12</sup> Notre traduction. Le terme original est « expectation ».

<sup>13</sup> Le D du R&D.

<sup>14</sup> « While expectations in their general form can be defined as the state of looking forward (from Latin, expectatio, looking, waiting for), technological expectations can more specifically be described as real-time representations of future technological situations and capabilities. » (Borup, Brown, Konrad & Lente, 2006 p. 285)

<sup>15</sup> Le schéma est ici utilisé afin d'offrir une idée de la localisation du « Fuzzy Front End ». Nous lui reconnaissons cependant le défaut de présenter le processus de conception de manière linéaire.



Tableau 1. Différence entre Fuzzy Front End et développement d'un nouveau produit (Reid & de Brentani, 2004 notre traduction)

	<b>Fuzzy Front End</b>	<b>New Product Development</b>
<b>Nature du travail</b>	Expérimental, souvent chaotique. Moments « Eureka ». Le travail peut être planifié mais pas l'invention.	Discipliné et orienté-objectif (« goal-oriented ») avec un plan de projet.
<b>Mise sur le marché</b>	Imprédictible ou incertaine	Haut degré de certitude
<b>Financement</b>	Variable – possibilité de travail en perruque pour certains projets, financements pour d'autres.	Budgété
<b>Attentes en termes de génération de revenu</b>	Souvent incertaines, avec une forte dose de spéculations	Prédictibles, avec un degré de certitude, d'analyse et de documentation croissantes à mesure que la date de sortie du produit approche.
<b>Activité</b>	Les individus et les équipes qui conduisent la recherche minimisent le risque et optimisent le potentiel.	Produit multifonction et/ou équipe de développement des process
<b>Evaluation des progrès</b>	Concepts renforcés	Réussite d'une étape clé

L'intensification de la course à l'innovation, trait saillant de la « *modernité tardive* », a pour résultante la déportation, en amont de la diffusion des technologies, des problématiques liées à leur adéquation aux caractéristiques des terreaux d'accueil envisagés. La nécessité de remonter jusqu'à la phase du « *Fuzzy Front End* » se fait de plus en plus exigence (Cooper, Robert G. & Kleinschmidt, 1993). Dans le secteur des TICs, la

vulgarisation de leur utilisation dans les sociétés occidentales, l'extension de leurs supports d'intégration et l'amplification de leurs capacités d'intercommunication<sup>16</sup> ont des conséquences importantes sur l'allocation des rôles au sein des filières impliquées. En effet, la forte intensité concurrentielle du secteur brouille de plus en plus la distinction entre les filières de production, reposant sur les avantages escomptés de l'innovation, et les filières de consommation, reposant sur l'identification des besoins en aval de la diffusion. Le rythme effréné imposé par la concurrence encourage ainsi moins l'adoption d'une stratégie d'adaptation aux *besoins* du marché que la conception de produits et services façonnant le marché. Ainsi, cette convergence des priorités d'orientation des stratégies à adopter (production/consommation) a eu pour répercussion notable l'irradiation de ces problématiques à des secteurs auparavant peu concernés par celles-ci. Ainsi en est-il pour des industriels du secteur des TICs qui étaient, au mieux, rompus aux réflexions stratégiques du marché industriel, sinon aiguillés par les agendas de R&D. Ces industriels reconnaissent aujourd'hui l'absolue nécessité d'intégrer des préoccupations *grand public* dans leurs stratégies. La réflexion sur le devenir des productions issues de la R&D, en somme sur l'innovation, est ainsi devenue la préoccupation de tous dans la filière des TICs : chaque acteur de la filière a à cœur de pouvoir anticiper les débouchés potentiels des innovations afin d'adapter, avant la concurrence, recherche, développement et production de produits attractifs pour le *grand public*, qu'il s'agisse de produits finaux ou de composantes technologiques à forte valeur ajoutée destinées à être intégrées à d'autres produits. Ce constat, qui n'est au fond qu'une actualisation des résultats de la nouvelle sociologie des sciences<sup>17</sup>, a amené certains laboratoires de recherche industrielle à dépasser le stade réflexif en le formalisant dans leurs structures organisationnelles. La reconnaissance du « Fuzzy Front End » de l'innovation comme le lieu privilégié d'élaboration de la matière originelle de l'innovation, le lieu où s'élabore la « *ligne de recherche* » (Vergragt, 1988) du processus de conception, est ainsi actée.

Or, c'est sur ce chemin cahoteux que se déplacent les recherches spéculatives pour l'innovation lorsque voix au chapitre leur est accordée : entre intensité réflexive et injonction à innover, elles ouvrent de nouveaux espaces de pratiques susceptibles d'ébranler

<sup>16</sup> « Information technology is changing from only being tools for the researcher or the business professional to becoming part of our everyday lives. Part of this change is due to the rapid development of inexpensive embedded, wearable, and mobile computing systems and the continuous miniaturization of components that allow us to create a range of novel computational artifacts at a reasonable cost. This technological development and its implications for how we both think about and design human-computer interaction have been the starting point for several lines of research in recent years such as ubiquitous computing [Want et al. 1995; Weiser 1991], tangible media [Ishii and Ullmer 1997], and augmented reality [Wellner et al. 1993]. » (Hallnäs and Redström 2002: 107)

<sup>17</sup> Voir infra.

les frontières de territoires balisés<sup>18</sup>. Cette pratique de la sociologie est d'autant plus intéressante qu'elle est privée d'« *hindsight*<sup>19</sup> » et d'« *obduracy* ». La pression à formuler des diagnostics tendant vers l'inférence et respectant le principe de véridiction<sup>20</sup> se couple à l'handicap d'une pratique démunie de sujets agissants (qui observer ?), de social existant (quelles interactions observer ?), voire d'impératif hypothétique clair (pour quoi et pour qui observer ?). Le FFE rend chacun de ces termes fugaces. Néanmoins, les méthodologies déployées n'éclosent pas du vide. Elles oscillent entre les techniques propres aux protocoles expérimentaux<sup>21</sup>, les méthodes d'enquête sociologique et d'autres sources d'inspiration méthodologique (cf. Figure 2)<sup>22</sup>. Il plane comme un « *air de famille*<sup>23</sup> » avec les pratiques d'investigation traditionnelles (voir Chapitre V pour un exemple détaillé). De l'expérimentation, ces méthodologies empruntent la variabilité des cadres d'investigation au sein d'une même étude et la volonté de contrôler l'effet de ceux-ci à des fins d'interprétation et de manipulation des résultats. De l'enquête sociologique, ressort la volonté de généralisation latente des résultats obtenus à partir de l'observation et de l'analyse des réponses d'un échantillon d'individus (Matalon & Ghiglione, 1998). Ce sont ces pratiques, qui parfois inspirent des gestes d'humeur ou de répugnance vifs<sup>24</sup> et se trouvent indubitablement en proie à la « *tentation du prophétisme* » (Bourdieu, Chamboredon & Passeron, 1983), qui sont au cœur de notre investigation. Nous souhaitons contribuer à la

<sup>18</sup> « But I can see now, at the end of 1999, that there is a common ground, a new territory being formed by the reciprocal respect between designers and the social scientists. It is clear that social science still has much to offer design, just as design has much to offer the social sciences. In participatory experiences, the roles of the designer and the researcher blur and the user becomes a critical component of the process. The new rules call for new tools. » (Sanders, 2002 p. 4)

<sup>19</sup> Nous traduisons ce terme par sagesse rétrospective. « For we are able to say that technical objects changed, stabilized, naturalized, or depoliticized social relations only with the benefit of hindsight. It is only after the event that causes are stabilized. And it is only after the event that we are able to say that objects do this, while human beings do that. It is in this sense, and only in this sense, that technical objects build our history for us and «impose» certain frameworks. And it is only for this reason that an anthropology of technology is both possible and necessary. » (Akrich, 1992 p. 222) Notre idée fait également écho à ce que Pierre Bourdieu appelle le privilège de la totalisation : « la capacité de se donner et de donner la vue synoptique de la totalité et de l'unité des relations qui est la condition du déchiffrement adéquat. » (Bourdieu, 1980 p. 138-139)

<sup>20</sup> (cf. page 16)

<sup>21</sup> « La langue française emploie un seul mot pour exprimer les deux acceptions de ce terme : l'expérience. Pour la science, l'expérience signifie, en général, observation provoquée et mesurée, ce que les Allemands nomment *Experiment*. Pour les philosophes et le sens commun, l'expérience c'est le fait d'éprouver quelque chose, en tant que ce fait apparaît comme un phénomène transitoire qui agrandit et enrichit notre pensée. C'est l'*Erfahrung* des allemands. De là vient, on ne l'a pas suffisamment noté, qu'on ne se soucie pas de distinguer entre ces deux significations et que l'on passe allègrement de l'une à l'autre. [...] Afin d'éviter toute ambiguïté, disons que la méthode expérimentale est conçue comme l'expérience, dans le premier sens d'observation mesurée et provoquée. » (Moscovici & Pérez, 2003 p. 60)

<sup>22</sup> Pour aller plus loin, on pourra également se reporter à (Löwgren & Stolterman, 2004 ; Ljungbald, 2008)

<sup>23</sup> Wittgenstein désigne par ce terme des ressemblances dont on ne parvient pas à établir l'élément qui crée la ressemblance. Les membres d'une même famille peuvent tous avoir un « air de famille » sans pour autant qu'on puisse déterminer ce qui fait qu'ils ont tous cet air de famille. La diversité d'usage des mots, leur vague plus ou moins grand tiennent à ce que les utilisations d'un mot ne présentent entre elles que des « ressemblances de famille » : « un réseau complexe d'analogies qui s'entrecroisent » sans qu'« une chose soit commune à ces phénomènes ». (Jaffro & Labrune, 1996 p. 797)

<sup>24</sup> « Malgré leurs nombreuses différences, [la sociologie expérimentale] et [la sociologie sociale] partagent néanmoins des détestations communes. Par exemple, parce qu'il a perdu toute velléité critique en se mettant au service des pouvoirs (point de vue critique du sociologue social) et parce qu'il a perdu toute autonomie scientifique et toute perspective de connaissance pour devenir un « homme d'action » ou au service de l'action (point de vue critique du sociologue expérimental), le « sociologue d'institution » (sociologue d'entreprise, sociologue d'Etat, conseiller des princes...), qui revendique une utilité et une prise sur le réel contre tous les « idéalistes » refusant d'affronter les réalités du pouvoir, est, comme l'« artiste bourgeois », mis au banc de la sociologie par ces deux courants. » (Lahire, 2002 p. 51)

réflexion entamée sur les professions, les métiers et les positions expertes de ces praticiens (Trépos, 2001 ; Legrand & Vrancken, 2004 ; Piriou, 2006) en questionnant directement les pratiques associées. La démarche est conforme à celles des entreprises ethnographiques d'analyse et d'observation de pratiques ingénierales, comme processus sociotechniques contingents (Bucciarelli, 1994 ; Vinck & Laureillard, 1996 ; Vinck, 2003) : l'objectif est d'entrer dans la matière de pratiques quotidiennes faite d'objets, d'hommes et de médiations (Vinck, 2003) qui s'exercent au contact des sciences pour l'ingénieur, à l'épreuve d'une modernité réflexive et au service de l'innovation technologique. Il est donc possible que cette thèse laisse un goût d'inachevé en ce qu'elle n'attaque pas frontalement la définition des frontières de la sociologie<sup>25</sup>, ni celle des frontières de la science (Gieryn, 1983) et qu'elle aborde de manière encore plus oblique les problématiques liées à l'économie du pouvoir et des légitimités (Winner, 1980 ; Hard, 1993 ; Rip, Misa & Schot, 1995 ; Bell, David, 2006). La modification des champs de forces qui sous-tend l'instrumentalisation de la sociologie en pratique n'est cependant pas niée ici : ce travail se veut également contribution à une meilleure compréhension de l'objet de dispute que constituent ces pratiques. En outre, notre thèse laisse dans l'ombre les préoccupations éthiques de la conception technologique (Winner, 1993 ; Radder, 1996 ; Feenberg, 2004). L'idée du bien et du mal, de ce que devrait être une bonne technologie ou une bonne pratique de conception, ne sauraient être totalement absentes mais, ici, elles ne constituent pas l'objectif premier de la production de connaissances.

Cependant, nous nous attaquons bien à l'autre versant des politiques des technologies (Berg, 1998), soit le fait de s'interroger sur une technologie de production de connaissances en tant qu'ordonnancement de collectifs sociaux où le social est appréhendé d'une manière étendue<sup>26</sup>. En effet, le paradoxe de la modernité tient à ce que sur le même front aient lieu un

<sup>25</sup> Nous refusons, ce faisant, le positionnement radical de Bernard Lahire qui hiérarchise les interrogations que l'on peut avoir sur la sociologie : « Or, sachant que l'utilité extra-scientifique de la sociologie dépend en partie de sa reconnaissance sociale en tant que discours scientifique légitime, il est clair que plus la sociologie atteindra un haut degré de rigueur scientifique et plus elle pourra escompter avoir du poids dans un monde social qui place (encore ?) très haut la production de vérités de type scientifique. Avant de répondre à la question : « à quoi sert la sociologie ? », il faudrait donc être capable de répondre à l'interrogation plus fondamentale : « Qu'est-ce qui définit la sociologie et le hors-sociologie ? » Accepter, de façon faussement démocratique, que le meilleur et le pire se côtoient au sein de cette discipline, est le meilleur moyen de perdre toute légitimité collective et, du même coup, toute utilité sociale. » (Lahire, 2002 p. 44). Ainsi, en s'intéressant à des pratiques adossées à la sociologie comme science, nous avons choisi de ne revenir directement sur la question du « Boundary Work » qu'en conclusion de notre étude.

<sup>26</sup> « We need to remind ourselves that when we talk of the technological, we are not talking of the “purely” technological—that no such beast exists. Rather we are saying that the technological is social. Already, then, we find that we need to blur the boundaries of categories that are normally kept apart. There is no real way of distinguishing between a world of engineering on the one hand and a world of social on the other. But this is only the first difficulty, for the word “social” presents us with analogous problems. What do we mean when we write of the “social”? Do we mean “social” as in “sociological”? The answer is that we do, but only in part. For the social is not exclusively sociological. In the context of technology and its social shaping, it is also political, economic, psychological—and indeed historical. » (Bijker & Law, 1992 p. 6)

processus de purification (simplification, classement, mise en ordre du monde) créateur de zones ontologiques différenciées (homme/femme, nature/culture, science/technique) et un processus de traduction producteur d'hybrides troublant les typologies préalablement établies (Latour, 1991). De là vient notre initiative à examiner ces recherches spéculatives comme des technologies à part entière dont on voudrait « ouvrir la boîte noire », selon la formule consacrée en sociologie de la technologie.

Notre initiative participe de la critique formulée par le sociologue Steve Woolgar à l'encontre de ceux qui traitent de la technologie, objet alors nouveau de la sociologie des sciences, à l'aide de la métaphore textuelle (Woolgar, 1991). Dans cet article, l'auteur constate que la sociologie des techniques repose sur la même critique post-kuhnienne des préconceptions que celle qui fonde la sociologie de la connaissance scientifique<sup>27</sup>. Cependant, il note que la critique du déterminisme technique<sup>28</sup> tend à s'appuyer sur des modes d'explications causales qui impliquent la possibilité de décrire les caractéristiques essentielles d'une entité technologique. Or, ces modes d'explication vont à l'encontre du principe de flexibilité interprétative<sup>29</sup> en prenant pour acquis les caractéristiques d'une technologie ou en décidant de soumettre certaines technologies au principe tandis que d'autres ne sont pas questionnées.

Cette application sélective du principe de flexibilité interprétative tout comme celle des bases théoriques de la sociologie de la connaissance ne sont pas seulement critiquées au regard de l'horizon empirique que se donne l'analyste. En effet, Woolgar s'attaque également à la mise à distance de l'objet de l'enquête (notamment le technologue) du sujet de l'enquête, l'analyste. Ce processus est inhérent à la production de « *mobiles immuables*<sup>30</sup> » (Latour, 1987), de « *technologies de représentations* » (Woolgar, 1991) que

---

<sup>27</sup> « Distinctions between the technical [scientific] and the social must be broken down. Social analysis should attend to the content of technology [scientific knowledge]. The role of the great individual engineer, inventor [scientist, discoverer] must be seen in social context. Technological [scientific] growth can no longer be thought of as a linear accumulation of artifacts [facts], each extrapolated from an existing corpus of technological achievement [scientific knowledge]. In short, technology [science] involves process as well as product, and technological artifacts [scientific facts] are to be understood as social constructs. » (Woolgar, 1991 p. 24)

<sup>28</sup> C'est-à-dire le fait de penser la technologie comme en dehors de la société, activité indépendante qui découle de l'application des découvertes scientifiques, qui, verticalement, ont un impact sur le reste de la société.

<sup>29</sup> « Demonstrating the interpretive flexibility of an artifact amounts to showing that one seemingly unambiguous "thing" (a technical process, or some material contraption of metal, wood, and rubber as in the case of the bicycle) is better understood as several different artifacts. Each of the different artifacts hidden within that seemingly one "thing" can be traced by identifying the meanings attributed by the relevant social groups. The concept of interpretative flexibility is crucial in countering technical determinism. Indeed, to recognize the interpretative flexibility of artifacts is synonymous with refuting technical determinism. Hence the concept's key role in the social studies of technology: Technical development can be subjected to social analysis only when it can be seen as being not autonomous and not driven by purely internal dynamics. The use of the concept of interpretative flexibility is thus the *raison d'être* of the social studies of technology, the justification for its existence. » (Pinch, 1993 p. 118)

<sup>30</sup> Ils ont pour propriété d'être aussi mobiles qu'immuables, présentables, lisibles et combinables avec d'autres objets. A l'exemple de la carte géographique, elles conservent leurs formes (immuables) tandis qu'elles circulent dans le temps et l'espace (mobile). « [...] il faut faire venir le monde en certains points qui deviennent alors des centres ou des points de passage obligé. Très bien, mais sous quelle forme faire venir le monde pour que, d'une part, ce qui est loin, distant et

constituent les productions de la recherche en sciences sociales : articles, ouvrages, supports de présentations et, bien sur, thèses. Or, ces technologies de représentations réduisent au silence l'objet des enquêtes qu'elles portent : les technologies de représentations ainsi que leurs concepteurs, une fois l'investigation achevée et couchée sur papier, n'ont plus d'espace pour répliquer. La voix de l'analyste prime sur celles des actants qu'il a observés. Ainsi, la production du sociologue échappe au champ d'application de la flexibilité interprétative alors que cette production participe de la représentation des technologies étudiées.

Pour contrecarrer cette faiblesse de la sociologie des techniques, Woolgar propose d'aller jusqu'au bout de la métaphore de la technologie comme texte. Il reconnaît les apports d'une approche instrumentale de la métaphore (Latour, 1987 ; Bijker, Hugues & Pinch, 1989 ; Bijker & Law, 1992) qui souligne le fait que l'identité de la technologie se construit durant sa conception. Les concepteurs se livrent ainsi bataille pour stabiliser certaines formes de lecture de la technologie : ce sont eux, les lecteurs du texte, qui en façonnent le sens privilégié durant son élaboration. Ces études, en retraçant la pluralité des chemins qu'auraient pu emprunter une technologie désormais stabilisée, mettent en lumière les liens entre un environnement et le processus de développement technologique. Woolgar reproche à cette approche instrumentale le fait que l'analyste, en décrivant le destin d'un parcours technologique, est tenté de privilégier une lecture qui, loin d'être neutre, coïncide avec les objectifs analytiques de celui-ci. Ainsi, la variété des champs des possibles est mise en lumière afin de servir les intérêts, avoués ou non, de l'analyste.

Woolgar reconnaît par ailleurs les apports d'une approche interprétativiste qui vise à répondre à la question des lectures différenciées des technologies. En sus d'étudier le pourquoi et le comment de ces lectures différenciées, cette approche permet de comprendre les raisons pour lesquelles une lecture est plus plausible qu'une autre en déplaçant l'observation vers l'usage de ces technologies<sup>31</sup>. S'il considère que cette approche pêche moins que la précédente, du fait qu'elle prolonge l'indétermination des technologies au-delà de la phase de conception, Woolgar considère néanmoins qu'elle n'échappe pas à la critique précédente : le compte-rendu de l'analyste prime sur ceux des actants.

---

périssable, s'y trouve assemblé, et que, d'autre part, le centre ainsi constitué ne soit pas un formidable embouteillage ? Il faut inventer des dispositifs qui mobilisent les objets du monde, maintiennent leur forme et puissent s'inspecter du regard. Il faut surtout que toutes ces formes puissent se combiner à loisir et se retravailler de telle sorte que celui qui les accumule dispose d'un surcroît de pouvoir. Alors, et alors seulement, certains points deviennent des centres capables de dominer sur une grande échelle. Dans la suite des recherches, je ne parlerai plus des lieux où se cumulent les mobiles immuables que comme des centres de calcul, sans plus m'occuper de savoir à quels domaines ces calculs ressortissent. » (Latour, 2006 p. 33-34).

<sup>31</sup> (Oudshoorn & Pinch, 2005)

Figure 2. Vue d'ensemble des méthodes de recherche spéculatives et estimation de leurs valeurs respectives pour chaque discipline (Sciences sociales (SS), gestionnaires (B), ingénieurs (E) et designers (D)). (Stewart & Claeys, 2009)

Method	Description	Comments	Outputs	Value for disciplines
<i>Cultural probes</i>	Designer technique, creative contextual investigation method.	Do things that SS would take for granted.	Pictures, beautiful probe material, drawings, movies	SS: generic info B: nice visual material for in presentations E: not really interesting nor useful D: love it
<i>Participant Observation</i>	Contextual investigation. Observing practices in naturalistic environment. Aiming at giving new viewpoints to the topic.	Not valuable without literature research in advance. Very time consuming and sometime hard to negotiate access, especially when in private or sensitive environments	Pictures, diaries, discussions,	SS: core methods for in depth study and theory development B: not very valuable E: really check D: background material > designer like it more to work with (individual) people, and if observing, then in lab context.
<i>Participative design / co-design</i>	Taking seriously input of 'users' – tapping into non-expert's ability to invent and imagine possibilities of technology.	Usually limited to generating ideas by users (e.g. by brainstorming) to use during the use case definition phase or new ideas on design level rather than on application or experience level.	Paper prototypes, pictures, ideas	SS: type of participant observation, but worries about influencing process. B: nice visual material E: new ideas (for features) D: new design ideas
<i>Scenario building with users</i>	Business and engineering tool to define requirements, offer simple range of choices and means to balance risks and potential.	Involves choosing limited number of factors (e.g. 2) and organising ideas and data. If done quickly cannot incorporate careful researched information	scenarios	SS: seem simplistic and reductionist, don't know what to do with it B: need it to define business model and choices E: use it for requirement definition D: imagination tool
<i>Long interviews</i>	Qualitative Social Science method	Very time-consuming, especially when wanting to analyse it properly	Texts, quotes	SS: research report exploring meanings and practices through talk. B: quotes for use in business pitch E: over complex material D: useful insights, but not creative, visual or tactile
<i>Focus groups</i>	Marketing and now Social science method bring a range of 'users' together. Can be a panel of unknowns, or people who know each other well (e.g. family).	Hard to run, and limited in what it can cover, but very illuminating as ideas, practices etc. are challenged in group and not by researcher.	Recordings, videos, texts	SS: explore meanings and alternative perspectives B: get range of views and opinions quickly E: get range of views and opinions quickly, especially on experiences with prototypes D: as above
<i>Interventions</i>	Creating events or objects that would not normally be part of an environment or everyday activities in order to challenge participants, stimulate critical thinking and conversations.	A strong design element, very much aimed at stimulating the critical and inventive of the participants, but unlike cultural probes, often done in dialogue with the creator. Can be lengthy to set up and analyze. Actually similar to user testing, but not focused on validating the object.	Texts, videos, images	SS: Not a usual method, but used in Action Research, or in asking for Interpretations of texts, images. B: very vague, not as concrete as direct feedback on products E: D: an important human-centred design method, drawn from the arts.
<i>Surveys</i>	Quantitative Social Science method.	Very expensive to do, therefore often done on small scale, useless output then.	Report, statistics, models	SS: find it interesting when representative part of the population is studied. B: love it, numbers is what they want E: believe it, it's a model D: mostly used for usability research

Woolgar propose une troisième manière d'aborder la métaphore en adoptant une approche réflexive qui consiste à mettre en équivalence la textualité des technologies observées et celle des arguments déployés dans l'analyse. Selon l'auteur, la technologie n'agit pas seulement à distance de l'analyste, mais se construit également dans la relation de l'analyste à son objet<sup>32</sup>. Cette relation, mise à distance dans les approches instrumentales et interprétativistes<sup>33</sup>, impose sa proximité dans l'élaboration de notre propre texte. En ayant pour objet les « *recherches spéculatives pour l'innovation* », notre investigation participe dès lors d'un vertige réflexif. D'abord, parce que ces pratiques sont insérées dans l'économie de production scientifique et participent donc, en tant qu'objet d'étude, du champ de la sociologie des sciences et des techniques. Ensuite, parce qu'en décidant d'investiguer sociologiquement une pratique de la sociologie, le texte étudié se fait très proche du texte analytique. Enfin, parce qu'en considérant cette pratique comme une technologie, nous choisissons de délaisser l'objectif de catégorisation entre sociologie et pratique de la sociologie, entre science et technologie afin de saisir au mieux la fabrique de ces pratiques « *centrées sur l'acceptabilité des technologies, et sous-tendues par un objectif de rationalisation* » et qui s'interrogent sur les manières de « *réinvestir l'élucidation de ce que les gens font au nom de ce qu'ils croient dans la production de dispositifs « adaptés » aux usages, ou dans la diffusion de savoirs sociaux qui projettent dans les dispositifs des valeurs dont on espère qu'elles capteront « l'énergie croyante » des usagers.* » (Le Marec, 2001 p. 141). La distance de l'objet au sujet se réduit donc à la fois du fait de la nature de l'objet et de l'intention de l'enquête. Ces deux facteurs justifient l'adoption d'une posture ethnographique visant ni à expliquer ni à distinguer mais à élucider la performance<sup>34</sup> de ces technologies dans leur environnement (Vinck, 2003). L'accent est ainsi mis sur les médiations et les pratiques effectives des acteurs humains et non humains afin de suivre au plus près les associations générées et éprouvées par l'incorporation des recherches

<sup>32</sup> « This is done by reducing (perhaps removing) the distance interjected between analyst and object when the latter is viewed as a realm of practice essentially different from that of (the analyst's) argument. Under this rubric, what we apprehend as technology is to be construed as text, the production and consumption of which is on a par with our own writing and reading practices. In other words, our analysis starts from the position that the textuality of technologies and the textuality of argument is essentially similar. » (Woolgar, 1991 p. 39)

<sup>33</sup> « In describing (accounting for) technologies as the product of objects or forces outside ourselves, we underplay the sense in which we are enmeshed in the web of associations that makes technology what it appears to be. In particular, by attempting to explain technology, we are in danger of explaining it away, precisely in the sense that the technology becomes an object disengaged from the author and subject only to "social forces" apparently removed from the world of the analyst. The reflexive construal of technology as text is an attempt to interrogate in the web of associations through which our apprehension of technology is ordinarily constrained. In short, technology is to be understood not just as a text that acts at a distance on its authors but as an entity that acquires this feature through only the relationships constituted in our own texts. » (Woolgar, 1991 p. 43)

<sup>34</sup> « [Our project] also attempts to explain performance – i.e., what is actually produced through human activity. Our theory is that performance, aside from technical or functional elements that can be explained by natural sciences or mathematics, is contingent on human behavior and language. Performance, like meaning, is something that ethnography can help us understand. » (Vinck, 2003 p. 208)



spéculatives pour l'innovation aux processus de conception situés dans le Fuzzy Front End de l'innovation. Notre problématique apparaît alors plus clairement ici :

*Comment les recherches spéculatives pour l'innovation, technologies particulières de réduction de l'incertitude planant sur le développement de l'innovation technologique, s'inscrivent concrètement dans les étapes amont des processus de conception ?*

Les questions qui forment le sous-bassement de la problématique de notre thèse sont ainsi les suivantes :

Quelles politiques, au sens d'ordonnancement de collectifs, sont mises en œuvre par les recherches spéculatives pour l'innovation ? Quelle est la performance de ces collectifs durant l'activité de conception ? Quelle est la performance de l'activité de conception en FFE sur le façonnage des recherches spéculatives ? Comment s'arrangent ces recherches situées entre les contraintes et les contingences de l'activité de conception comme processus contingent de construction sociotechnique et celles de la pratique de la sociologie, encouragée à la formulation de diagnostics, de l'inférence et du principe de véridiction ?

Afin d'éprouver ces questions, nous avons choisi de prendre comme point d'appui empirique des « projets de R&D » réalisés dans le tissu industriel grenoblois. La production de cette thèse doit être comprise comme s'insérant au sein d'un réseau rhônalpin dense et pluridisciplinaire de chercheurs en sciences sociales intéressés à la question du savoir scientifique et de sa place dans nos sociétés. Ce travail, qui a bénéficié de l'appui financier et scientifique de la région Rhône Alpes, participe donc d'une tradition d'associations polymorphes entre science, industrie et sciences sociales dans la région. Empiriquement, cet attachement s'est traduit par l'encadrement de la thèse par une praticienne de la sociologie professionnellement engagée en tant que telle auprès d'un acteur industriel majeur, le CEA-LETI<sup>35</sup>. Ce centre de recherche appliquée en microélectronique et en technologies de l'information et de la santé est situé au cœur du Campus d'innovation MINATEC, premier campus européen de micro et nanotechnologies principalement initié par le CEA et l'Institut National Polytechnique de Grenoble (INPG). Ce campus, inauguré en juin 2006, accueille environ 4000 personnes (2400 chercheurs, 1200 étudiants et 600 industriels) et concentre les acteurs majeurs de la filière de la microélectronique, soit l'étude et la fabrication de composants électroniques à l'échelle micronique et désormais à l'échelle nanométrique. Le CEA-LETI est depuis environ trente ans soumis aux contraintes de l'hypercompétitivité et

---

<sup>35</sup> Le CEA est un établissement de recherche à caractère scientifique, technique et industriel. C'est un Etablissement Public à caractère Industriel et Commercial (EPIC). Le LETI est le Laboratoire d'Electronique et d'Instrumentation du CEA.

du capitalisme d'innovation intensive. Alors qu'il était déjà investi d'une mission qui se démarquait de celle d'autres laboratoires gouvernementaux<sup>36</sup>, le CEA-LETI fait désormais pleinement partie de ces organisations décrites plus haut : le passage de l'invention à l'innovation nécessite une prise en compte précoce des préoccupations des destinataires des produits au sein desquels les composants développés par le CEA-LETI sont amenés à être intégrés. Le laboratoire se trouve ainsi engagé dans une « *ligne de recherche qui se rapproche de plus en plus du grand public* » (Vinck, 2007) tandis que son activité est elle-même située dans le Fuzzy Front End de l'innovation.

C'est dans ce contexte que les sciences sociales ont été introduites au CEA, en particulier à Minatec et au CEA-LETI. L'organisation qui pave la voie de cette intégration est le MINATEC IDEAs Laboratory®, plateau d'innovation multipartenaires chargé d'imaginer de nouveaux produits et de nouveaux services intégrant micros et nanotechnologies. Il a été créé en 2003 à partir d'une réflexion initiée en 1998 et compte le CEA, France Telecom et ST Microelectronics comme membres fondateurs. Ils sont rejoints en 2004 par Essilor International et l'Université Pierre Mendès France puis par Rossignol (fabricant de sport de montagne), Teamlog (développeur de logiciel) et l'Université Stendhal avant qu'EDF et d'autres industriels s'y associent à partir de 2006. Trois pôles d'activités sont présents : un pôle créativité, un pôle de développement de maquette et un pôle consacré aux usages des TICs. Dès 2007, trois nouvelles structures éclosent.

Tout d'abord, l'atelier Arts-Science, lieu commun d'expérimentation et de fertilisation croisée entre scientifiques et artistes, est créé en 2007. L'atelier cristallise institutionnellement une collaboration initiée en 2002 entre l'Hexagone de Meylan et le CEA à travers les « Rencontres-i, festival des imaginaires », événement culturel annuel organisant des rencontres entre artistes, scientifiques et entreprises. L'atelier travaille à la collaboration entre chercheurs, ingénieurs et artistes dans le but d'intégrer les technologies développées par le CEA dans les productions artistiques et d'enrichir les processus de créativité des participants. Il s'agit également de profiter de cette fertilisation croisée pour provoquer de nouveaux questionnements et aborder d'un autre angle le débat science-société. L'atelier est hébergé dans le bâtiment du MINATEC IDEAs Laboratory®, situé à l'orée du CEA.

---

<sup>36</sup> « la mission est moins de produire de la connaissance académique que de mettre au point des concepts opérationnels et les savoir-faire associés destinés à des utilisateurs intermédiaires, industriels notamment, mettant au point de nouveaux produits ou services. » (Vinck, 2007 p. 94)

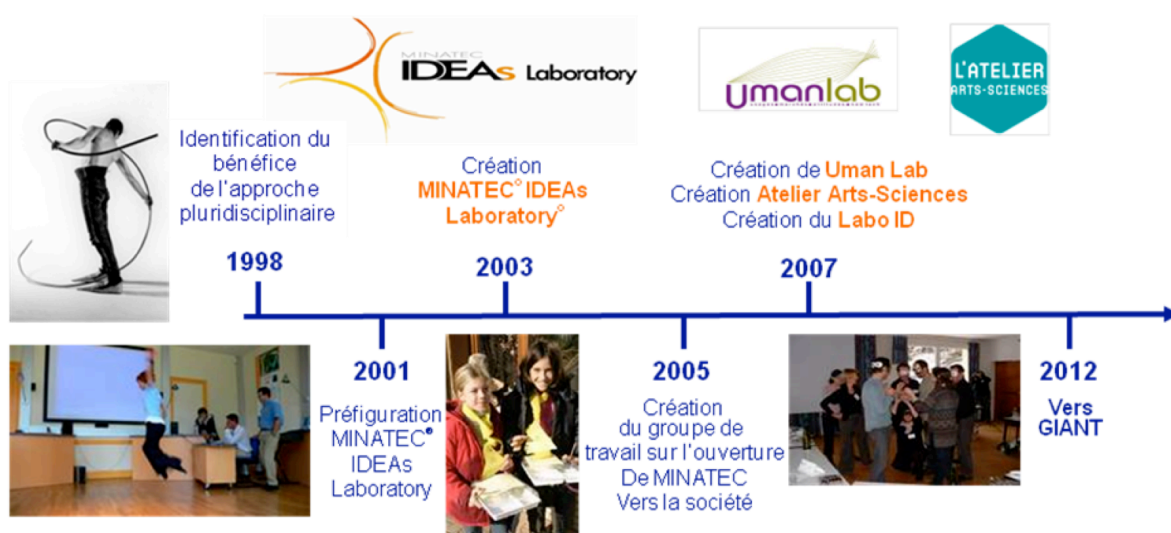
Hébergée dans les locaux du CEA-LETI, Umanlab est une équipe de recherche technologique de l'Université Pierre Mendès France, adossée scientifiquement au laboratoire Pacte, reconnue par le Ministère de la recherche et de l'enseignement supérieur pour la période 2007-2010 (ERT 65). Alors que la plupart des ERT sont jusqu'ici souvent mono-disciplinaires et agissent dans le champ des sciences et technologies, le projet Umanlab entend regrouper des compétences pluridisciplinaires en SHS pour accompagner les développements technologiques, en particulier dans le contexte du pôle scientifique Minatec et du CEA-LETI. Umanlab a pour vocation le développement de méthodes, transférables au monde industriel, permettant d'accompagner les programmes d'innovation d'exploration. Les partenaires de l'équipe Umanlab sont les premiers bénéficiaires de ces développements. Ces méthodes s'appuient sur des approches de scénarios (mise en scène d'usages futurs imaginés), d'expérimentation d'usages potentiels avec des prototypes de la technologie, de modélisation et de simulation de situations stratégiques, ou encore de micro-segmentation des marchés. L'ERT a pour partenaires, l'UPMF, l'IEP Grenoble, Grenoble INP, Grenoble Ecole de Management, l'Université Stendhal, le CEA, Minatec, le MINATEC IDEAs Laboratory®, EDF, Schneider Electric Electric, la SNCF, Predictys (start-up spécialisée dans l'optimisation des campagnes email-marketing) et Crowdspirit (plateforme de crowdsourcing qui permet aux entreprises d'impliquer des innovateurs extérieurs dans la conception de produits et services innovants)<sup>37</sup>.

Créé en 2008, le LID est un laboratoire dont l'offre comme la compétence sont intégrées à celles des équipes Systèmes en cohérence avec les missions du Service Microsystèmes et Objets Communicants (SMOC) au sommet de la pyramide du CEA-LETI. Il œuvre pour des projets internes au CEA ou alors développés de manière bilatérale avec des industriels. Composé à sa fondation d'anciens membres du MINATEC IDEAs Laboratory®, le LID est présent dans les projets développés au sein du MINATEC IDEAs Laboratory®, de Umanlab et de l'atelier Arts-Sciences. Le travail s'articule autour de trois axes de connaissance et d'action : l'usage, la créativité dans la conception technologique ainsi que la médiation avec la société civile. 80% de l'activité du LID est dédiée au support opérationnel de projets de conception technologique et 20% consacrés à la recherche en lien avec les domaines de compétences du CEA-LETI<sup>38</sup>. C'est au sein de cette structure que nous avons été hébergés et que nous avons pu avoir accès à une multitude de projets, soit en tant que praticien de la sociologie soit en tant que simple observateur.

<sup>37</sup> Le recensement des partenaires s'est fait après consultation du site internet de Umanlab (<http://www.umanlab.com/>). Les différences de statut ou de contributions entre partenaires dans Umanlab ne sont ici pas reflétées.

<sup>38</sup> Source : rapport d'activité 2008 du CEA-LETI.

Figure 3. Historique de l'introduction des SHS à Minatec (tiré d'un transparent de présentation de l'institution auprès du Conseil Economique et Social en juillet 2008)



Notre investigation s'est appuyée, en partie, sur notre participation à l'un de ces projets qui intégraient des recherches spéculatives et impliquaient des partenaires issus de champs disciplinaires divers. Ce sont des lieux où les acteurs se réunissent, discutent, échangent, mettent au pot commun, s'accordent autour d'objets, à travers les médiations. Ces projets de conception exploratoire ont nourri notre réflexion jusqu'à se constituer comme matériau d'investigation, comme terrains empiriques faits, c'est-à-dire existants et fabriqués, pour convenir à notre posture de recherche. Cette conception du terrain emprunte à une approche communicationnelle de la pratique notamment construite sur une pensée réflexive de pratique de la sociologie des usages (Le Marec, 2002 ; Le Marec & Babou, 2003). Le terrain<sup>39</sup> est ainsi compris comme un lieu doté d'une pertinence pour les acteurs mais également comme un objet « *reconfiguré par la recherche, borné cette fois-ci par les contraintes théoriques et empiriques* ». Le choix des projets de R&D multipartenaires s'explique ainsi par la volonté de travailler sur des unités qui, en sus de répondre à nos objectifs de recherche, constituent des situations qui articulent ces deux définitions du terrain. Cette volonté satisfait aussi à l'exigence d'adoption d'une posture ethnographique et réflexive. Joëlle le Marec et Igor Babou ont développé à cet égard le concept

<sup>39</sup> « Le terrain devient alors une catégorie complexe structurée par le rapport entre les communications sociales instrumentalisées pour les besoins de l'enquête, et les communications sociales constituées en données ou en objets. C'est ainsi que le terrain est d'abord un lieu qui a une pertinence sociale comme lieu de pratiques qui se mettent volontairement en rapport les unes avec les autres. On peut discriminer ce qui est terrain au sens d'unité spatiale et temporelle socialement pertinente du point de vue des acteurs qui la vivent comme telle (une bibliothèque, une école), et ce qui est terrain au sens d'unité d'observation de phénomènes pertinents du point de vue du chercheur. » (Le Marec, 2004 p. 145)

méthodologico-théorique de « *composite* », outil d'observation situé entre l'anthropologie et la sémiotique :

*« Les configurations hétérogènes et dynamiques que nous qualifions de « composites » décrivent des situations de travail au sein desquelles des individus mobilisent à la fois des objets matériels et des représentations (priméité), réalisent des actions (secondéité) et mettent en oeuvre des systèmes de normes ou des règles opératoires (tiercéité). Un composite caractérise un ensemble de processus sociaux, techniques et sémiotiques mobilisés dans le cadre d'une tâche professionnelle décrite par les acteurs et observée à travers les objets qui sont produits ou manipulés à cette occasion. Ces composites constituent donc un objet construit par la recherche, défini a priori, qui nous permet de déplacer la notion d'usage en élargissant les dimensions prises en compte, tout en restant opératoire par la focalisation sur une tâche précise, les différentes tâches professionnelles décrites par les bibliothécaires. » (Le Marec, 2002 p. 187)*

Dans ce travail, nous en conservons plus l'esprit qu'une application à la lettre. En effet, en choisissant le projet comme terrain, l'objectif est de se donner les moyens « *de ne pas détruire les phénomènes de conception* » que l'on souhaite étudier, les recherches spéculatives pour l'innovation. Les relations entre les textes<sup>40</sup> observés et les textes de l'analyse sont maintenues à travers les pratiques qui peuplent les projets<sup>41</sup>. Ces pratiques de la sociologie sont autant pertinentes pour les acteurs (praticiens de la sociologie et autres membres des projets) que pour nous-mêmes, en tant qu'analyste (pratiques lues comme des recherches spéculatives pour l'innovation situées au croisement de deux modernités). Notre intégration aux projets en tant que praticien de la sociologie renforce ce lien communicationnel entre les deux acceptions du terrain en nous plaçant sur le chemin de crête de ceux-ci : entre pratique de recherche doctorale, pratiques de la sociologie et pratiques de conception technologique.

En effet, notre terrain a été choisi pour sa capacité à apporter des réponses à notre problématique. Ainsi, la première partie de la thèse participe de l'expérience d'immersion dans les réseaux au sein desquels circulent ces praticiens de la sociologie. Ces réseaux s'étendent sur plusieurs dimensions : historique, économique, scientifique, professionnelle et personnelle. Ces liens sociaux, dont la prégnance s'est affirmée au fil de ce travail, s'ils ne se croisent pas tous, tournent tous autour de la notion d'« usage » de TICs. Parce que la

---

<sup>40</sup> au sens de Woolgar.

<sup>41</sup> « Les composites se distinguent de notions voisines comme celle de *média* et de *dispositif* car ils sont avant tout des savoirs incarnés dans des situations et des relations entre objets, discours et représentations. Ils sont proches de la notion de *texte* [...] » (Le Marec & Babou, 2003)

notion est vissée aux recherches spéculatives dont nous nous saisissons, nous avons choisi d'explorer les rapports de ces pratiques de la sociologie à l'« usage ». En restant fidèle à la conception de la sociologie des sciences et des techniques, nous avons voulu éviter autant que faire se peut la rationalisation *a posteriori* de l'histoire de la notion. Nous avons donc préféré restituer de manière dynamique l'une des trajectoires du concept, de sa genèse à son instrumentalisation hors champ académique jusqu'à sa mobilisation dans le champ des recherches spéculatives pour l'innovation. A l'aide du concept beckerien de déviance, trois idéaux-types des rapports entretenus entre la notion et ses manipulateurs ont ainsi été dégagés comme autant de mises en lumière de l'historicité du concept. Notre objet de recherche s'est ainsi construit au regard de cette trajectoire et a été conquis par la proposition d'une définition provisoire, celle de la *projection d'usage*, qui va servir de fil conducteur à notre investigation.

La seconde partie de la thèse est consacrée à la justification de l'approche méthodologique choisie ainsi qu'à l'intérêt de concentrer l'analyse sur le scénario d'usage. Nous démontrons que la projection d'usage, dans le Fuzzy Front End de l'innovation, est le premier pas vers la stabilisation de l'innovation. Nous aborderons ensuite la scénarisation comme l'une des modalités de la projection en recensant avec un regard critique les différentes formes d'utilisations des scénarios d'usage. Nous retracerons les différentes formes d'usage du scénario dans le champ de la conception afin d'en définir les contours pluriels avant d'en justifier l'étude par sa qualité d'« *objet intermédiaire de conception* » (Jeantet, 1998 p. 325). Nous concluons cette partie en explicitant l'adoption de l'observation participante comme mode d'investigation par l'ambition de suivre au plus près le travail de projection d'usage ainsi que par les contraintes imposées par le terrain.

La troisième partie de la thèse est une entrée de plain-pied dans le champ empirique : le projet COPRIM (COnтактless Privacy Manager). Nous y avons été associés en tant que praticien de la sociologie, par le biais de la participation de Umanlab au projet. Dans cette partie, nous nous concentrons sur le scénario, produit de la projection d'usage. Nous démontrerons que l'ancrage de celui-ci dans les codes de la fiction fait du scénario un ensemble d'actes de langage performatifs et vraisemblables ainsi qu'un acte de croyance qui lie l'ensemble de ces promoteurs.

Dans la quatrième partie, nous explorons la construction d'une projection d'usage à travers l'analyse d'élaboration de scénarios d'usage de TICs en conception. L'objectif n'est pas seulement de montrer que les choses ne se sont pas déroulées comme prévues mais bien de proposer une lecture des spécificités des performances de la conception de projection

d'usage : dynamiques performantes dans, par et avec les objets, les personnes et les médiations. Nous démontrerons, à cet effet, que la projection d'usage est une forme de stabilisation de l'incertitude mais qu'elle ne constitue pas un énoncé scientifique. La projection d'usage se situe dans le champ des *axiomes* en ce qu'elle autorise la possibilité d'un travail scientifique au prix de déplacements d'identités de ceux (humains et non humains) qui la produisent. Enfin, nous revenons sur la teneur réflexive intrinsèque à notre investigation comme lieu de convergence entre terrain, chercheur et les médiations entre ceux-ci. Nous revisitons, à cette occasion, notre travail (le terrain, nous-mêmes et les médiations associées) à l'aide de la notion de *composition* qui permet notamment de mettre à jour l'arrière-plan analytique de cette étude.

## Partie 1. L'usage, carrières d'un concept<sup>1</sup>

---

<sup>1</sup> Cette partie a permis d'alimenter l'écriture d'un chapitre dans l'ouvrage dirigée par Dominique Vinck et Bernard Miège : *Les masques de la convergence. Enquêtes sur sciences, industries et aménagements* (2012). Sous le titre *L'oeuf vient en premier...dans la question. L'exemple du concept d'usage : point de fuites et de convergences disciplinaires*, ce chapitre fait l'objet d'une discussion dans l'ouvrage (Bernard Miège) qui a permis l'amélioration sensible de l'écriture de cette partie.



*«« Technology is assumed to be designed, developed, and produced by engineers. They are at the drawing boards and behind the laboratory benches; they apply for patents, model the prototype, and test in the pilot plant; they show the newly born artifact to the press and, if lucky, they figure prominently in the glossy photographs of stories about heroic inventors. Once these engineers have produced the technology, it is passed on to the sales people, the managers, the trade, and, finally, to the users. Engineers design technology, managers produce it, salespeople sell it, tradespeople distribute it, users use it. Alas, this neat and orderly image of technical development, so pervasive in all but the most recent technology studies, is not only too simple—  
it is wrong. »*

*Bijker, W., « The Social Construction of Fluorescent Lighting, or How an Artifact Was invented in Its Diffusion Stage », in Bijker, W. et Law, J. (éd.) (1992). *Shaping Technology/Building Society*, Cambridge, London, The MIT Press, p. 75-102.*

Proche collaboratrice de Michel de Certeau, Luce Giard offre au lecteur un éclairage précieux sur le contexte qui a vu émerger la réflexion de l'intellectuel sur les « *arts de faire* ». Dans sa présentation au recueil princeps de Michel de Certeau, *L'invention au quotidien* (1990), l'historienne nous fait apprécier la frondeur de l'esprit à l'origine de cette initiative de recherche. *L'invention au quotidien* résulte d'une commande du service des études et recherches au Secrétariat d'Etat à la Culture. Il s'agissait d'un contrat de recherche intitulé « Conjoncture, synthèse et prospective » qui a duré de 1974 à 1977. Tandis que de Certeau et son équipe bénéficiaient des résultats d'une grande enquête sur les pratiques culturelles des français, inspirée des approches diffusionnistes et fonctionnalistes (Rogers, Everett M. & Shoemaker, 1971) alors dominantes dans la sociologie des usages<sup>42</sup>, ils ont fait le choix de se démarquer de la méthodologie quantitative alors prisee par les prospectivistes<sup>43</sup> et portent leur attention aux formes d'inventivité des cultures populaires dans leurs pratiques quotidiennes. Ce déplacement nourrit un renversement dont l'amplitude débord sur d'autres projets, objets et disciplines académiques et conduit à des déplacements théoriques et méthodologiques radicaux. La notion d'autonomie, soit la capacité des individus à se montrer créatifs dans leur confrontation à l'offre de biens ou de services qui leur est proposée, bascule en tête de l'agenda de recherche d'un champ alors en constitution, celui de la sociologie dite « *des usages*<sup>44</sup> ». Un déplacement dont on retrouve l'essence dans cette citation :

*« Producteurs méconnus, les consommateurs produisent par leurs pratiques signifiantes quelque chose qui pourrait avoir la figure des « lignes d'erre » dessinées par les jeunes autistes de F. Deligny. Dans l'espace technocratiquement bâti, écrit et fonctionnalisé où ils circulent, leurs trajectoires forment des phrases imprévisibles, des « traverses » en*

<sup>42</sup> La sociologie des usages est issue d'un basculement qui s'est produit au sein de la sociologie des médias avec les travaux des chercheurs américains, dans les années 1960-1970. A cette époque, le paradigme dominant consiste à étudier les « effets » et l'« impact » des médias sur les gens et leurs opinions. Ils s'interrogent notamment sur l'ampleur des effets (forts selon les chercheurs de l'école de Francfort ou faibles selon Lazarsfeld) des outils de communication. Avec Rogers et le courant « uses and gratifications », il s'agit de s'arracher au média-centrisme dominant pour porter son attention sur ce que les gens font avec les médias. L'hypothèse est que les personnes ne reçoivent pas passivement les messages et qu'elles ne sont pas conditionnées par les médias mais qu'elles utilisent ces médias pour en tirer des satisfactions et des compensations psychologiques. Cette approche fonctionnaliste de la relation aux outils de communication constitue une rupture par rapport au déterminisme technique des médias et de leurs effets sur la société. Elle constitue une nouvelle tradition influente dans les années 1970 qui construit des catégories d'utilisateurs, procède à des études quantitatives et prospectives dans le domaine des politiques culturelles.

<sup>43</sup> « Ce n'est pas qu'il méprise les chiffres, mais une telle démarche laisse échapper tout ce qui l'intéresse : les opérations et les usages individuels, les enchaînements et les trajectoires changeantes des pratiquants. » (De Certeau, 1990 p. x; présentation de Luce Giard)

<sup>44</sup> On trouvera souvent dans la littérature rattachée à ce champ une filiation établie avec le projet de de Certeau. Si le nombre élevé de références dont il fait l'objet témoigne de la vigueur et de la pérennité de sa pensée, ce serait faire un raccourci que de considérer que sa théorie des pratiques a immédiatement joué un rôle structurant dans ce champ de recherche. En réalité, la diffusion large de l'œuvre de de Certeau tient d'abord à la proximité des thématiques qu'il explore avec celles des chercheurs intéressés par l'étude de l'usage des TICs (Le Marec, 2004). Ainsi, l'introduction de cette première partie de thèse participe autant d'un biais des conditions d'investigations que d'une volonté d'instruire la question de l'usage à travers certains traits saillants.

*partie illisibles. Bien qu'elles soient composées avec les vocabulaires de langues reçues et qu'elles restent soumises à des syntaxes prescrites, elles tracent les ruses d'intérêts autres et de désirs qui ne sont ni déterminés ni captés par les systèmes où elles se développent. Même la statistique n'en connaît presque rien, puisqu'elle se contente de classer, calculer et mettre en tableaux les unités « lexicales » dont ces trajectoires sont composées mais à quoi elles ne se réduisent pas, et de le faire en fonction de catégories et de taxinomies qui lui sont propres. Elle saisit le matériau de ces pratiques, et non leur forme ; elle repère les éléments utilisés, et non le « phrasé » dû au bricolage, à l'inventivité « artisanale », à la discursivité qui combinent ces éléments tous « reçus » et couleur muraille. » (De Certeau, 1990 p. XLV)*

Cette attention accordée aux formes d'inventivité des cultures populaires, à l'élucidation du déploiement de « ruses », de « braconnages » et de « sens tactique » dans les pratiques quotidiennes<sup>45</sup> (l'espace, la lecture, les croyances) est caractéristique du « collège invisible », qui en réalité n'est pas l'apanage des sociologues<sup>46</sup>, et qui a pour objet et point de fixation l'usage des technologies de l'information et de la communication (TICs). Josiane Jouët (2000) attribue à l'étude sur l'usage du magnétoscope menée par Mallein, Baboulin et Gaudin (1983) un rôle inaugural dans l'ouverture de ce champ dont notre terrain constitue l'une des ramifications.

Le concept d'« usage » a été jusqu'ici évoqué sans être clairement défini<sup>47</sup>. Avant d'entrer plus avant dans l'analyse, nous avons souhaité tirer profit de sa richesse sémantique pour mieux circonscrire la dimension à laquelle nous nous attaquons dans cette thèse. Pour ce faire, nous nous appuyons sur le travail de Serge Proulx (2005) qui, en ambitionnant la construction d'une théorie des usages, a mis à jour une typologie de cinq catégories

<sup>45</sup> « J'appelle stratégie le calcul (ou la manipulation) des rapports de forces qui devient possible à partir du moment où un sujet de vouloir et de pouvoir (une entreprise, une armée, une cité, une institution scientifique) est isolable. Elle postule un lieu susceptible d'être circonscrit comme un propre et d'être la base d'où gérer les relations avec une extériorité de cibles ou de menaces (les clients ou les concurrents, les ennemis, la campagne autour de la ville, les objectifs et objets de la recherche, etc.). Comme dans le management, toute rationalisation « stratégique » s'attache d'abord à distinguer d'un « environnement » un « propre », c'est-à-dire le lieu du pouvoir et du vouloir propres [...] j'appelle tactique l'action calculée que détermine l'absence d'un propre. Alors aucune délimitation de l'extériorité ne lui fournit la condition d'une autonomie. Aussi doit-elle jouer avec le terrain qui lui est imposé tel que l'organise la loi d'une force étrangère. Elle n'a pas les moyens de se tenir en elle-même, à distance, dans une position de retrait, de prévision et de rassemblement de soi : elle est mouvement « à l'intérieur du champ de vision de l'ennemi », comme le disait von Bülow, et dans l'espace contrôlé par lui. Elle n'a donc pas la possibilité de se donner un projet global ni de totaliser l'adversaire dans un espace distinct, visible et objectivable. Elle fait du coup par coup. Elle profite des « occasions » et en dépend, sans base où stocker des bénéfices, augmenter un propre et prévoir des sorties. Ce qu'elle gagne ne se garde pas. Ce non-lieu lui permet sans doute la mobilité, mais dans une docilité aux aléas du temps, pour saisir au vol les possibilités qu'offre un instant. Il lui faut utiliser, vigilante, les failles que les conjonctures particulières ouvrent dans la surveillance du pouvoir propriétaire. Elle y braconne. Elle y crée des surprises. Il lui est possible d'être là où on ne l'attend pas. Elle est ruse. En somme, c'est un art du faible. » (De Certeau, p. 60. 61)

<sup>46</sup> (voir infra)

<sup>47</sup> Alain Chambat souligne le caractère vain d'une telle entreprise : « Alors que la question des usages occupe une place importante, voire croissante, dans la sociologie des TIC, le contenu et le statut théorique de la notion sont loin de faire consensus. Il serait vain de prétendre en apporter ici une définition, car sa signification résulte d'options théoriques qui la dépassent : elle participe en effet de débats qui opposent, en sociologie, l'agent et l'acteur, les niveaux micro et macro, la technique et le social, l'empirisme et la théorie critique. » (Chambat, 1994 p. 263)

analytiques distinctes pouvant aider à l'interprétation du concept. L'« usage » y est pensé en fonction du poids de l'histoire et contextualisé à différents niveaux organisationnels.

- Le premier niveau est « *l'interaction dialogique entre utilisateur et dispositif technique* » : il renvoie à l'analyse des interactions directes entre hommes et machines (HCI-Human Computer Interaction) avec un usage d'abord pensé comme « contraint par l'offre industrielle ».
- Le deuxième niveau est la « *coordination entre usager et concepteur du dispositif* » : il renvoie au travail de conception des interfaces et au domaine de l'ergonomie cognitive.
- Le troisième niveau est « *la situation de l'usage dans un contexte de pratiques* » : l'usage est ici envisagé dans un contexte de pratiques sociales et des rapports sociaux agissant la vie quotidienne.
- Le quatrième niveau est « *l'inscription de dimensions politiques et morales dans le design de l'objet technique et dans la configuration de l'usager* » : l'usage est envisagé au regard des valeurs morales et/ou politiques que portent les TICs, comme, selon la formule de Latour, technologie continuateur de la politique par d'autres moyens.
- Enfin, le cinquième niveau est « *l'ancrage social et historique des usages dans un ensemble de macrostructures* »

L'apport analytique de cette typologie pour la compréhension du caractère multidimensionnel des lieux d'élaboration de l'usage est indéniable. Cependant, l'opération de construction de notre objet de recherche a troublé le jeu de démarcation des cinq niveaux identifiés. Le centre névralgique de notre investigation résiste à une affiliation univoque à l'un des cinq niveaux: il se déploie plutôt sur une ligne parallèle au « *continuum de définition* » qui caractérise la notion d'« usage » (Breton & Proulx, 2002), ligne balisée par les centres d'intérêts et les disciplines des chercheurs impliqués. Nous le verrons plus tard, notre objet de recherche emprunte, à intensités diverses et avec une fidélité fluctuante, aux pôles d'intérêts identifiés. Cependant, formuler l'hybridité de notre objet d'un ton axiomatique ne nous dispense guère d'aller plus loin dans la délimitation de celui-ci.

Nous avons comme objectif initial l'établissement d'une « définition provisoire », « destinée à engager la recherche, à déterminer la chose à étudier, sans anticiper sur les

*résultats de l'étude* » (Mauss, 1968 p. 386)<sup>48</sup> et à préciser le type de « recherche spéculative » auquel nous souhaitons nous intéresser. Cependant, l'honnêteté intellectuelle nous oblige ici à confesser certaines prises de liberté avec les règles énoncées par Marcel Mauss. Ces écarts à la norme sont justifiés, non par la volonté d'innover ou de se démarquer des enseignements de l'anthropologue, mais par les contraintes posées par notre objet ainsi que par le rapport particulier entretenu avec celui-ci.

En effet, les contours de notre objet ne nous sont apparus clairement qu'après une longue période (environ un an) d'observation et d'intégration au sein des structures censées pratiquer l'usage d'une manière différente. Plus brutalement, cette année s'est révélée comme étape de préparation au véritable coup d'envoi du travail de recherche. Elle a permis d'instruire la fécondité ainsi que l'écologie de notre terrain : il s'agissait de trouver où, quoi et comment chercher. En cela, le déroulé de l'investigation se détachait déjà des impératifs maussiens en ce que l'extériorité et l'objectivité qui doivent présider à la construction de la définition<sup>49</sup> ont été entachées par notre immersion prolongée en milieu observé ainsi que par les impressions qui en résultaient. Ainsi, le lancement de l'activité de recherche a participé d'une modification profonde du rapport entre notre objet et nous-mêmes. Ces liens nous sont apparus d'une « inquiétante étrangeté » (« Das Unheimliche ») pour reprendre la formule freudienne : à mesure que nous nous familiarisions avec l'environnement au sein duquel circulait notre objet de recherche, celui-ci nous apparaissait de plus en plus étrange et suspicieux<sup>50</sup>. Ce paradoxe constitutif du sentiment d'inquiétante étrangeté, qui s'alimente de la confrontation d'une historicité individuelle et d'un ordre social et représentationnel particulier (voir infra.), a jeté les bases de l'élaboration d'une définition provisoire. Celle-ci n'intervint alors pas à proprement dit au début de l'entreprise de recherche. Ici, contrairement à ce qui est préconisé par Mauss<sup>51</sup>, la définition proposée n'a pas été construite préalablement à sa soumission à l'épreuve empirique. Elle a participé des prémisses de l'investigation empirique ; elle est un *commencement de preuve* des résultats de celle-ci.

---

<sup>48</sup> On regardera également (Durkheim, 1895)

<sup>49</sup> « Puisque cette définition vient au début de la recherche, c'est-à-dire à un moment où les faits sont seulement connus du dehors, elle ne peut être faite que d'après des signes extérieurs, il s'agit exclusivement de délimiter l'objet de l'étude et par conséquent d'en marquer les contours. Ce qu'il faut trouver, c'est quelques caractères apparents, suffisamment sensibles qui permettent de reconnaître, presque à première vue, tout ce qui est prière. Mais d'un autre côté ces mêmes caractères doivent être objectifs. Il ne faut s'en fier ni à nos impressions ni à nos prénotions, ni à celles des milieux observés. » (Mauss, 1968 p. 387)

<sup>50</sup> « Nous voilà avertis, en somme, que le mot « heimlich » n'a pas un seul et même sens, mais qu'il appartient à deux groupes de représentations qui, sans être opposés, sont cependant très éloignés l'un de l'autre : celui de ce qui est familier, confortable, et celui de ce qui est caché, dissimulé. » (Freud, 1919 p. 11)

<sup>51</sup> « En d'autres termes, c'est l'investigation empirique qui, pour l'essentiel, décidera soit que la définition proposée était heuristique, soit qu'elle était mauvaise et viciait toute la suite du raisonnement, ou qu'on a négligé tel fait qui entraînait dans la définition, ou bien enfin qu'on a fait entrer en ligne de compte des faits qui n'y entraient pas » (Mauss, 1968, 386)

L'avouer, c'est d'abord reconnaître la part de biais inhérent à notre démarche. Cela permet également de se prémunir contre toute tentative d'épurement *a posteriori* de la démarche de recherche. Enfin, c'est aussi un moyen d'expliquer que le soin particulier apporté à cette définition ne témoigne pas d'une recherche prise au piège de questionnements tautologiques mais participe de la complexité des relations entre l'objet et nous-mêmes. Dès lors, la prise de distance avec l'objet, entamée par les premières manifestations de cette inquiétante étrangeté, exigeait l'adoption d'une définition dont la précision et le détail anticipaient sur certains résultats de l'investigation sans pour autant en constituer des preuves complètes<sup>52</sup>. Ainsi, de nos premières observations, nous avons recherché le plus petit commun dénominateur des projections auxquelles nous étions confrontés. A chaque fois, nous avons donc pu observer la mise en scène de l'usage des technologies en conception. Cette mise en scène pouvait avoir des supports différents : il pouvait s'agir de films, d'animations flash, de scènes jouées in vivo, de récits écrits, etc. Aussi, systématiquement, les technologies en usage étaient intégrées dans une logique de récit impliquant l'interaction d'un grand nombre d'éléments : la technologie, bien sûr, mais aussi des personnages, leurs histoires, leurs intentions, leurs actions ; tous étant à un moment donné causes ou conséquences de modifications d'états ou d'actions de la technologie ou d'autres personnages, autrement dit de l'environnement spatio-temporel. En somme, l'usage était mis en système d'interactions au sens que lui donne la sociologie fonctionnaliste : la projection d'usage correspondait toujours à une mise en ordre du monde par la représentation des relations réciproques des choses qui peuplaient ces mondes. Ce dénominateur commun à l'ensemble de nos observations nous a permis d'élaborer une définition provisoire de la projection d'usage pour avancer dans notre investigation :

*C'est un travail de représentation de l'usage de technologie*<sup>53</sup>.

Cette définition a permis l'intensification des recherches de liens entre *projection d'usage* et « usage ». En effet, nous n'avons pas rencontré dans la littérature de développement ou de mise en lien éloquentes de l'idée de *projection d'usage* à celle d'« usage », bien que ce concept ait déjà été au centre de plusieurs analyses rétrospectives (Jouët, 2000 ; Le Marec, 2001 ; 2004 ; Bajolet, 2005 ; Jaureguiberry, 2008). Malgré leurs qualités respectives, le retour critique de Josiane Jouët, les réflexions théoriques de Joëlle le Marec, le panorama analytique d'Emilie Bajolet ou la récente contribution de Francis

<sup>52</sup> « Il n'est pas question, bien entendu, de définir d'emblée la substance même des faits. Une telle définition ne peut venir qu'au terme de la science, celle que nous avons à faire au début ne peut être que provisoire. [...] Mais cette définition pour être provisoire ne saurait être établie avec trop de soin, car elle dominera toute la suite du travail. Elle facilite en effet la recherche parce qu'elle limite le champ de l'observation. » (Mauss, 1968, 386).

<sup>53</sup> Cette première définition sera amendée au fil de la progression de la recherche.

Jaureguiberry n'établissent pas de généalogie entre la « sociologie des usages » et la *projection d'usage*. A minima, ce travail de projection est assimilé à un travail plus large, celui d'instrumentalisation du concept d'usage à des fins mercantiles ou économiques. Il serait néanmoins injuste de voir dans ce constat l'unique justification de notre initiative à traiter l'« usage » de manière originale. La direction prise par notre recherche a également été infléchie par le contexte au sein duquel il a été effectué.

Il est avéré que l'élaboration d'une revue de littérature, plus qu'une étape standard du travail scientifique, procède aussi d'une stratégie de recherche qui vise à qualifier le travail de contribution scientifique comme innovant, à plus forte raison lorsqu'il s'agit d'une thèse de doctorat. Ainsi, nous avons dépassé la littérature comme seule source d'inspiration et puisé dans notre expérience doctorale des éléments venus alimenter notre réflexion<sup>54</sup>. La fréquentation de divers lieux d'animation scientifique (séminaires, ateliers, colloques, conférences), en France comme à l'international, m'ont permis de prendre part à de nombreux échanges portant sur les tensions générées par la posture de praticien et l'exercice simultané d'un travail académique. Certaines de ces discussions, notamment lorsqu'elles impliquaient des tenants *historiques* de la « sociologie des usages », visaient à ce que je m'exprime sans équivoque sur la dimension politique qui entourait mon travail. En caricaturant à peine, la question posée était celle du camp dans lequel je me situais et conséquemment de l'endroit à partir duquel je m'exprimais : étais-je là pour défendre l'existence d'une sociologie praticienne en rupture plus ou moins affirmée avec la sociologie académique ou parlais-je au nom d'une forme critique de la sociologie en butte aux pressions exercées par le monde économique ? Cette incitation systématique à devoir prendre position n'eut longtemps pour effet que de m'obliger à adopter un mécanisme de défense discret et relatif au lieu et à la nature de l'injonction : défendre la probité du travail effectué par les praticiens sous les ors du monde académique ou se faire le héraut d'une sociologie critique lorsqu'attaquée au flanc par des représentants du monde industriel. Cependant, cette stratégie *ad hoc* et non réfléchie, bien qu'ayant prouvé une certaine efficacité pour couper court au débat, montrait rapidement ses limites lorsqu'examinée à la lumière de mes objectifs de recherche. C'est ainsi que mes réactions à ces échanges ont été à l'origine d'une lente réflexion personnelle sur la sociologie en tant qu'objet social : la nouvelle sociologie des sciences s'imposait comme ressource majeure, non seulement pour ma réflexion scientifique, mais également comme plateforme d'une démarche réflexive intense. Ainsi, il m'est apparu que les vives disputes qui sous-tendaient les échanges suscités

---

<sup>54</sup> L'usage de la première personne du singulier est utilisé à partir d'ici et durant les deux prochains paragraphes afin de souligner le caractère personnel des expériences relatées et des conclusions qui en sont tirées.

par ma présence visaient à la définition ou au rappel, d'un *bon* usage de la sociologie en prenant pour prétexte l'utilisation de l'« usage » comme concept sociologique et, bien entendu, comme objet social.

Cette prise de conscience tardive des enjeux politiques et éthiques qui entouraient mon travail de thèse s'est montrée d'une utilité redoutable dans le travail de construction de l'objet de recherche et de distanciation par rapport à mon terrain. L'« usage », d'acquis (« taken for granted ») se faisait conquête et objet de dispute. Cette compréhension-là permettait d'éviter l'écueil d'un évolutionnisme nécessairement partisan voyant dans les formes actuelles de manipulation de l'« usage » la conséquence d'une évolution logique et implacable des pratiques scientifiques et professionnelles. Par ailleurs, elle ouvrait la voie à une forme empathique de traitement de l'objet de recherche. En considérant l'« usage » comme un objet social, j'ai pu opérer une mise en abîme riche pour l'analyse. Tandis que la « sociologie des usages » dépeint la multiplicité de ceux-ci lorsqu'il s'agit d'objets sociaux singuliers, les TIC, la considération de l'« usage » comme un objet social ordinaire permet, en retour, d'appréhender la coexistence de plusieurs utilisations de celui-ci. Néanmoins, l'adoption d'une telle tactique de recherche n'a pu se faire en gommant le malaise ressenti durant mon travail.

C'est donc en postulant, d'abord, la variété des usages sociaux de l'« usage », que nous est apparu évidente la nécessité de considérer les formes d'existence sociale du concept. Ainsi, inspiré par le découpage analytique de Dominique Vinck pour analyser le travail scientifique, nous nous sommes penchés sur les différentes manières de comprendre la socialité de notre objet. Celle-ci s'exprime à travers les « institutions », les « collectifs », les « organisations », les « dynamiques sociales et les pratiques » qui font l'existence du concept (Vinck, 2007). Toutefois, cette analyse s'est rapidement imposée comme nécessaire mais insuffisante au vu de nos objectifs de recherche en ce qu'elle ne rendait pas intelligibles les fondements de la conflictualité latente qui opposent de manière dynamique ces usages sociaux. Afin de n'en pas perdre le bénéfice, nous avons choisi de l'associer à la notion de « déviance » développée par Howard Becker (1985) à partir de l'étude du monde des musiciens de jazz et de celle des fumeurs de marijuana :

*« Les groupes sociaux créent la déviance en instituant des normes dont la transgression constitue la déviance, en appliquant ces normes à certains individus et en les étiquetant comme déviants. De ce point de vue, la déviance n'est pas une qualité de l'acte commis par une personne, mais plutôt une conséquence de l'application, par les autres, de normes et de sanctions à un « transgresseur ». Le déviant est celui auquel cette étiquette a*



*été appliquée avec succès et le comportement déviant est celui auquel la communauté attache cette étiquette » (Becker, 1985 p. 32-33)*

Notre ambition est de démontrer la manière dont l'usage social<sup>55</sup> de l'« usage » a fait l'objet d'un processus d'étiquetage circulaire duquel la *projection d'usage* participe. En comprenant le concept d'« usage », d'ailleurs originellement déviant, comme situé dans une logique d'interactions avec le *social*<sup>56</sup> (institutions, collectifs, organisations, dynamiques et pratiques), nous nous donnons les moyens d'en lire les mutations en se dégageant de toute attitude normative. Dès lors, notre travail vise à comprendre comment l'« usage » a (été) généré (par)<sup>57</sup> des « *outsiders* » au double sens du terme : soit qu'ils aient transgressé une norme propre au groupe social dans laquelle cette norme est véhiculée ; soit/et qu'ils estiment que ce groupe et les « *entrepreneurs de morale*<sup>58</sup> » qui y sont associés sont étrangers à leurs propres mondes et sont eux-mêmes « *outsiders* ». La compréhension de la projection d'usage sera alors éclairée par le rétablissement d'une forme d'historicité à cette dynamique d'étiquetage qui tient en gravitation des êtres autour d'un concept mouvant.

Nous abordons cette question de l'usage social de l'« usage » à travers la notion associée de « *carrière* », processus de redéfinition de l'identité sociale à la fois du concept et de ceux qui le manient. Le concept de « *carrière* », emprunté à Hugues<sup>59</sup> (1958), est transposé dans l'étude de la déviance de manière heuristique pour décrire le cheminement par lequel un individu va se constituer comme déviant. Becker en distingue plusieurs étapes : la première est caractérisée par la transgression de la norme par le sujet ; dans la deuxième étape, la transgression se fait régulière et la déviance est socialisée ; elle fait l'objet d'une désignation publique dans un troisième temps avec l'acquisition chez l'individu d'un nouveau statut social ; enfin advient l'adhésion à un groupe de pairs qui génère l'élaboration de rationalisation légitimante de l'identité déviante et la perpétuation de pratiques et savoir-faire déviants. Afin d'épouser cette logique séquentielle, nous avons donc fait le choix de l'associer à l'analyse des formes de socialité scientifique identifiées plus haut.

---

<sup>55</sup> Ce qui revient à aborder l'usage comme une technologie.

<sup>56</sup> « La déviance est une propriété non du comportement lui-même, mais de l'interaction entre la personne qui commet l'acte et celles qui réagissent à cet acte. » (Becker, 1985 p. 38)

<sup>57</sup> « Ce ne sont pas les motivations déviantes qui conduisent au comportement déviant mais à l'inverse c'est le comportement déviant qui produit au fil du temps la motivation déviante. » (Becker, 1985 p. 64)

<sup>58</sup> « Les normes sont le produit de l'initiative de certains individus, et nous pouvons considérer ceux qui prennent de telles initiatives comme des entrepreneurs de morale. » (Becker, 1985 p. 171)

<sup>59</sup> « L'ensemble des relations sociales qui mettent aux prises les titulaires de rôles professionnels avec leurs clients, leurs collègues, ou d'autres groupes d'individus, et la manière dont ces relations affectent l'exercice de leurs activités » (Riutort, p.275)

Ainsi, le passage à l'acte nous permettra d'identifier la norme transgressée en abordant la question de l'institution, justifiée et légitimée à partir des ressources politiques que sont les normes (Barnes & Dolby, 1970 ; Mulkay, 1976). L'étape suivante, l'apprentissage social, sera abordée en analysant la manière dont les collectifs de déviants s'insèrent dans des axes de recherche et des marchés de diffusion dont le croisement assoit des régimes de recherche scientifique et technique (Pestre, 1997 ; Shinn, 2000). L'analyse du processus de désignation publique permettra de jeter un éclairage sur l'organisation du groupe de déviants, en tant que forme sociale « *qui assure la coordination des individus ou des groupes à une œuvre commune [...]* » renvoyant à « *un travail d'organisation débouchant sur une structure d'autorité, une division du travail et des mécanismes de coordination et de pilotage* » (Vinck, 2007 p. 92). Les dynamiques sociales à l'œuvre dans l'usage déviant de l'« usage » seront examinées du même pas au regard des cycles de crédibilité (Latour & Woolgar, 1979 ; Rip, 1994) et des types de réseaux au sein desquelles elles agissent (Vinck, 1992). Enfin, la question des pratiques sociales est abordée de manière transversale car celles-ci traversent chacune des étapes de la carrière de l'usage, dont elles fondent la déviance relative. Les pratiques propres au travail de projection d'usage feront l'objet d'un examen général, fondé sur la littérature, avant d'être plus développées dans la partie empirique de notre thèse<sup>60</sup>.

Nous avons donc opté pour une appréhension froide de l'« usage » en le *technicisant* dans l'analyse. Il s'agissait de le considérer comme un objet technique ordinaire, doté de destins pluriels, instrument de connaissance, de luttes définitionnelles et catégorielles, objet scientifique socialement construit, idéal-typique, à la fois fait et processus, qui s'efface en dernier lieu comme élément « naturalisé » par ces utilisateurs<sup>61</sup>, *taken for granted*. Ce faisant, nous avons identifié trois carrières au concept d'« usage » : *poiétique*, *pythique* et *sibylline*, chacune d'entre elles étant respectivement déclinée dans les trois chapitres suivants<sup>62</sup>.

<sup>60</sup> Voir Tableau 3, en fin de partie.

<sup>61</sup> « Once technical objects are stabilized, they become instruments of knowledge. Thus when an electricity company sets differential tariffs for high- and low-consuming domestic users, for workshops, and for industrial consumers, it finds ways of characterizing and identifying different social strata. If it also chooses categories used in other socioeconomic-political network, then the knowledge it produces can be “exported”. “Data” can thus be drawn from the network and transmitted elsewhere, for instance, to economists concerned with the relationship between the cost of energy or GNP and consumption. However, the conversion of sociotechnical facts into facts pure and simple depends on the ability to turn technical objects into black boxes. In other words, as they become indispensable, objects also have to efface themselves. » (Akrich, 1992 p. 221)

<sup>62</sup> Dans les lignes qui suivent, nous balayons un champ historique relativement large (au moins 30 ans) dont une phase d'intensification de la réflexion théorique (Jouët, 1993 ; Chambat, 1994 ; Flichy, 2003) sur l'usage postérieur aux échanges de données et aux retours sur expériences entre chercheurs, durant les années 1980, impulsés par la DGT (Direction Générale des Télécommunications) et le CNET (Centre National d'Etudes des Télécommunications), échangeant qui se poursuivent notamment dans la revue *Réseaux*. En vertu de la finalité de notre démonstration, à savoir le fait de retracer les carrières du concept d'usage, nous privilégions un compte rendu centré sur le concept et sur sa nature déviante et celles des

## I - L'usage, objet d'une pratique poïétique

---

Considérer l'« usage » comme un objet de *poïétique* traduit l'accent mis sur la capacité créative des utilisateurs de dispositifs technologiques par l'« école française des usages » (Jaureguiberry, 2008). De ce fait, l'« usage », objet scientifique politiquement chargé, brave l'establishment dominant de l'époque. En concentrant les efforts de recherche sur la mise en lumière des capacités créatives de l'usager, les chercheurs se sont livrés à la reconnaissance institutionnelle d'une véritable *poïétique*, comme « étude spécifique d'un faire producteur de quelque chose » (Ardoino, 1994). Cette pratique de l'usage s'inscrit ainsi dans la tradition d'un héritage aristotélicien, retravaillé par Paul Valéry<sup>63</sup>, dont la paternité du terme « poïétique » a été retracée par René Passeron (1989). Ce dernier élargit la focale de Valéry, centrée sur les conditions d'élaboration de la poésie, en comprenant l'art au sens aristotélicien de savoir-faire, comme un « faire producteur de quelque chose » :

« Nous proposons donc d'élargir la position de Valéry à tous les arts. Une perspective plus ambitieuse pourrait même l'élargir à toutes les œuvres de l'homme. On a parlé de l'homi viator, de l'homi ludens, de l'homme révolté, chacun y va de son interprétation de l'humain : comment nier que ce n'est plus par une ingénieuse doctrine, mais par une science humaine, liée à toutes les autres, qu'il faut montrer en quoi et de quelle façon l'homme est constructeur ? » (Passeron, René, 1989 p. 15)

Ainsi, toutes les activités humaines de création sont rattachées à la notion de *poiésis*, « faire producteur », dont la poïétique constitue l'étude. Dans ce chapitre, nous nous attacherons à démontrer que cette posture de recherche s'inscrit en faux contre une tendance dominante favorisant une prise en compte esthétique<sup>64</sup> de l'activité de l'usager. L'« usage » est étudié comme un construit social, mettant en jeu le sens tactique d'usager en prise avec la stratégie technicienne. Nous démontrerons que ce travail de réhabilitation de l'usage(r) s'est effectué par le travail d'un groupe de chercheurs provenant d'horizons disciplinaires et

---

communautés associées. Notre présentation ne cherche toutefois pas à rendre compte de la diversité des formes académiques d'exploration de l'usage dont les sources d'inspiration : courant diffusionniste, montée en puissance de l'ethnométhodologie, débats portants sur les forces et faiblesses de chaque approche disciplinaire, convergences entre sociologie de l'innovation et sociologie des usages, batailles pour remettre le « quotidien » au centre des débats. Le projet de ce chapitre est de rendre compte de la trajectoire du concept et de son devenir hors champ académique.

<sup>63</sup> « Un autre tas [que l'esthétique comme étude des sensations] assemblerait tout ce qui concerne la production des œuvres ; et une idée générale de l'action humaine complète, depuis ses racines psychiques et physiologiques, jusqu'à ses entreprises sur la matière ou sur les individus, permettrait de subdiviser ce second groupe, que je nommerais *Poétique*, ou plutôt *Poïétique*. D'une part, l'étude de l'invention et de la composition, le rôle du hasard, celui de la réflexion, celui de l'imitation ; celui de la culture et du milieu ; d'autre part, l'examen et l'analyse des techniques, procédés, instruments, matériaux, moyens et suppôts d'action. » (Valéry, 1957 p. 1331)

<sup>64</sup> « [...] la poïétique est la promotion philosophique des sciences de l'art qui se fait : pour elle, par exemple, la peinture est un phénomène d'atelier. Inversement, l'esthétique est la promotion philosophique des sciences de l'art qui se consomme. » (Passeron, René, 1989 p. 16)

institutionnels différents : « l'école française des usages », véritable « collège invisible », qui se structure autour de revues et colloques scientifiques importants. Enfin, nous décrivons la manière dont l'ancrage national de ce réseau « forum » de chercheurs a eu un retentissement au-delà des cercles académiques, succès qui porte les germes de l'usage pythique de l'« usage ».

### ***A - Le passage à l'acte déviant : l'usage, de la statistique au construit social***

Comme nous l'avons évoqué dans l'introduction, l'« école française des usages » s'est notamment construite sur le travail de requalification des usagers effectué par Michel de Certeau. Nous profitons ici du témoignage éclairé de Francis Jaureguiberry pour résumer cet état de fait :

*« L'école française des usages » s'empara de cette image des usagers décrits comme des “producteurs méconnus, poètes de leurs affaires, inventeurs silencieux de sentiers propres dans les jungles de rationalité fonctionnaliste” (De Certeau, 1990 p. 19) pour étudier comment “les procédures populaires jouent avec les mécanismes de la discipline et ne s'y conforment que pour les tourner” et pour montrer comment “ces manières de faire constituent les mille pratiques par lesquelles des utilisateurs se réapproprient l'espace organisé par les techniques de la production socioculturelle” (De Certeau, 1990 p. 14). » (Jaureguiberry, 2008 p. 32-33)*

Cette école s'est attachée à lire dans les écarts observés entre usages prescrits et usages effectifs des TIC, non des erreurs commises par les usagers, mais une zone dans laquelle peut se lire la créativité et l'inventivité de ceux-ci. Cette *poiësis* est exprimée à travers les notions de « bricolage » et de « braconnage » (De Certeau, 1990), de « sens tactique » (De Certeau, 1990), de « détournements » (Baboulin, Gaudin & Mallein, 1983 ; Boullier, 1984 ; Laulan, 1995) ou encore de « manières de faire » (Charon, 1992 ; Jouët, 1993 ; De Gournay, 1994) ; elle marque le fait que la reconnaissance de la compétence inventive de l'utilisateur participe du caractère transgressif de l'école des usages.

Le Minitel peut être regardé comme l'objet idoine de ce courant d'études. Bénéficiant d'une attention particulière de la part des chercheurs en sciences sociales (Boullier, 1984 ;

Mallein & Toussaint, 1985 ; Toussaint, 1992 ; 1992), cet objet va permettre de populariser l'intérêt d'une étude fine des usages effectifs dans les années 1980. En effet, durant les expérimentations menées, les chercheurs vont mettre en lumière le « sens tactique » des usagers du Minitel. D'une part, seul le service d'annuaire téléphonique est plébiscité par ceux-ci tandis que les autres services proposés, qui procédaient d'une volonté de rapprocher l'administration de ces administrés, sont délaissés. D'autre part, les possibilités techniques du Minitel ont été détournées par les usagers qui ont pris appui sur le réseau pour développer et utiliser des messageries conviviales interpersonnelles (le Minitel rose). Cet usage est et restera le plus répandu parmi tous<sup>65</sup>.

Au-delà de la réhabilitation de la parole de l'utilisateur ou de ses capacités d'action, c'est la rationalité techniciste qui, par le truchement des observations, prête le flanc à la critique (Chambat, 1994). Soit de manière voilée en raison de l'appartenance des chercheurs à des structures promouvant ces technologies, sinon de façon plus directe, à l'instar de Mallein et Toussaint dans un texte de dénonciation du déploiement de logiques de « *performance technosociale* » (Mallein & Toussaint, 1994). Celle-ci est, selon eux, caractérisée par quatre concepts : l'idéalisation (la TIC vise un public idéalisé pour une technologie parfaite), la substitution (la TIC va éradiquer les usages préexistants), la révolution (la TIC va déclencher une véritable révolution sociétale) et enfin la passivité (l'utilisateur n'a d'autre choix que l'exit ou la loyalty).

L'« école française des usages », par le biais de ses travaux, opèrent un véritable travail de sappe sur les fondations de ces postures technicistes en relevant et mettant à jour le processus de construction sociale à l'œuvre dans l'« usage ».

Ainsi, la dimension historique y tient une place importante, notamment par la prise en compte du poids des traditions, des habitudes qui permettent de comprendre, voire d'anticiper, l'inertie du corps social à modifier son comportement et ses pratiques de manière révolutionnaire (Perriault, 1989 ; Jouët, 1993 ; Scardigli, V., 1994 ; Scardigli, Victor, 1995). Les usages sont perçus comme procédant d'un antérieur à ne pas négliger :

« *L'observation des usages sociaux des TIC montre en effet la façon dont ils s'insèrent dans des pratiques familiales ou professionnelles préexistantes ou en voie de*

---

<sup>65</sup> On pourra lire à cet égard le très instructif roman d'Alexandre Bellanger, *La Théorie de l'information*, Gallimard, 2012.

*constitution. Les recherches démontrent qu'il n'existe pas d'usage sui generis et que l'adoption des technologies de l'information et de la communication s'articule autour de techniques et de pratiques antérieures. » (Jouët, 2000 p. 500)*

L'« usage » est ainsi envisagé dans une approche généalogique. Cette perspective évolutionniste offre une issue à l'appréhension statique de l'usage par la prise en compte et l'examen analytique des différentes phases qui concourent à la socialisation des TIC. Celles-ci sont donc examinées du point de vue de leur découverte, de leur adoption, du temps d'apprentissage requis mais aussi du point de vue de leur banalisation<sup>66</sup>. A cet égard, Emilie Bajolet a résumé ces phénomènes en trois « *moments-clés de la construction socio-technique des TIC* » :

*« D'abord le moment particulier qui correspond au passage entre l'usage idéal d'un outil technique, imaginé par ses concepteurs, et son usage effectif ; ensuite la période de diffusion d'un nouvel outil de communication, l'usage s'inscrivant alors dans une généalogie de pratiques préexistantes, ou filières socio-techniques ; enfin, le stade qui correspond à la rencontre entre la « machine à communiquer » et ses divers publics d'utilisateurs, celle-ci faisant alors l'objet d'appropriations matérielles, pratiques et symboliques contrastées. » (Bajolet, 2005 p. 51)*

De manière liée, les phénomènes de « filiation » entre technologies sont mis en évidence. Les annonces prophétiques de *tabula rasa* portées par les concepteurs sont révoquées par les observations faisant état de phénomènes d'hybridation entre TIC (machines à écrire et ordinateur, téléphone, Minitel et répondeur, courrier électronique et courrier papier, baladeur et chaîne hifi, etc.). Cette inscription de la TIC dans une écologie lui préexistant se manifeste, chez les utilisateurs, par une « *réduction de l'inconnu au connu*<sup>67</sup> » (Boullier, 1984).

Ce temps d'accueil de l'« usage » à l'intérieur duquel se nouent les liens entre le passé et le présent, l'existant et l'avenir, est également le lieu de construction du sens

---

<sup>66</sup> « De l'adoption à la banalisation, la construction de l'usage s'opère par étapes marquées par le désenchantement de la technique, par un rétrécissement des usages au regard des attentes initiales et des emplois frénétiques de la phase d'exploration, bref par son passage au statut d'objet d'ordinaire qui l'incorpore dans les pratiques sociales. » (Jouët, 2000 p. 501)

<sup>67</sup> « L'opération spontanée la plus fréquente pour réduire l'étrangeté de la présence de cette machine, pour stabiliser un environnement ébranlé, pour résoudre cette dissonance, consiste à attribuer à l'objet inconnu les propriétés d'objets déjà connus. Cette réduction de l'inconnu au connu fonctionne à l'analogie et produit le paradoxe selon lequel toute innovation, pour être intégrée, doit être dans un premier temps, niée comme telle et insérée dans une chaîne de significations (ici de produits et d'usages) déjà identifiées. » (Boullier, 1984 p. 82)

octroyé à la technique, et partant, de l'usage de celle-ci. L'adoption d'une approche constructiviste et compréhensive est partagée par l'ensemble des chercheurs qui relèvent l'importance des significations portées par les usagers sur la technique et ses usages<sup>68</sup>. Cette attention portée aux « significations d'usage » est le soubassement des travaux portant sur l'appropriation des TIC. En considérant celui-ci comme « un procès, l'acte de se constituer un *soi* » (Jouët, 2000 p. 502), les chercheurs s'autorisent l'exploration des dimensions subjectives et collectives de l'« usage »<sup>69</sup>.

Bien que Francis Jauréguiberry critique le manque de diversité des collectifs abordés dans les études portant sur l'appropriation<sup>70</sup>, les identités personnelle et sociale des individus enserrés dans ces collectifs ont fait l'objet de nombreux travaux qui démontrent à la fois le poids des variables socioculturelles dans le processus d'appropriation et le rôle que peuvent jouer les TIC dans la construction de l'identité sociale des individus. Aussi, ont été étudiés plus particulièrement certains groupes sociaux en fonction de l'âge, du genre, de l'organisation familiale, de la nationalité ou encore du statut professionnel (Breton, 1989 ; Kaufmann, 1995 ; Monjaret, 1996 ; Calogirou & Andre, 1997 ; Castelain-Meunier, 1997 ; Rivière, 2000 ; Eve & Smoreda, 2001 ; Lelong & Thomas, 2001).

Un autre versant du processus d'appropriation suscite un foisonnement de recherches. Il s'agit de la dimension *cognitive* et *empirique* qui aborde plus matériellement la relation de l'utilisateur au TIC :

« *Sa construction met en jeu des processus d'acquisition de savoirs (découverte de la logique et des fonctionnalités de l'objet), de savoir-faire (apprentissage des codes et du mode opératoire de la machine), et d'habilités pratiques.* » (Jouët, 2000 p. 502)

Cette dimension est marquée d'un double mouvement d'« *acculturation de la technique* » par l'usage et d'« *empreinte de la technique* » sur celui-ci (Jouët, 1993). Dans

---

<sup>68</sup> « La socialisation d'une technique dépend moins de ses soi-disant caractéristiques intrinsèques ou de sa sophistication technique que des possibilités qu'elle offre à une intégration dans l'ensemble des significations sociales, culturelles et imaginaires de modes de vie. Or, l'évolution de ceux-ci est très largement dépendante de variables qui débordent de toute part le cadre de la pensée technicienne dans lequel cette technique a été nécessairement conçue. » (Mallein & Toussaint, 1975 p. 153)

<sup>69</sup> Les chercheurs du CETCOPRA, laboratoire pratiquant une véritable sociologie de l'appropriation, distingue trois niveaux d'étude de ce processus : « Au niveau individuel, l'utilisateur agit de façon à ce que l'innovation convienne à sa personnalité : il l'intègre dans ses schèmes perceptivo-moteurs familiers, ses habitudes de travail et son expérience antérieure (...). Plus globalement, il organise l'ensemble de ses objets techniques quotidiens pour leur donner un sens personnel, lié à la trame de sa propre vie : comme s'il réalisait une 'mise en intrigue' de l'innovation, pour parler comme Paul Ricœur ». À celui du groupe d'appartenance, où les cultures de métier, des classes d'âge et de milieux jouent un rôle fondamental. Et enfin à celui de la culture, au sens géographique de culture régionale ou nationale. » (Gras, Moricot, Poirot-Delpech & Scardigli, 1994 p. 261-262).

<sup>70</sup> « Peu en effet se focalisèrent sur les modes de vie, les micro-cultures, les styles et modes de distinction, les genres liés au sexe ou à l'appartenance ethnique. » (Jaureguiberry, 2008 p. 36)

le premier processus, l'utilisateur doit se plier aux impératifs techniques de TIC porteurs de valeurs spécifiques (rationalité, performance, ordre), tandis que dans le second, ce sont « *les mobiles, les formes d'usage et le sens accordé à la pratique* » qui sont envisagés en tant qu'ils « *se ressource dans le corps social.* » (Jouët, 1993).

Nous avons donc jusqu'ici identifié les traits saillants qui caractérisent les travaux de l'« école française des usages » (rôle productif de l'utilisateur, le delta entre usages prescrits et usages effectifs, l'importance du temps dans la construction des usages et le caractère socialement construits de ceux-ci) (Chambat, 1994). Cependant, pour frondeuse qu'elle soit, cette manière d'aborder l'usage ne constitue pas une remise en cause des « normes éthiques » dans la communauté de chercheurs concernés<sup>71</sup>. Ce sont plutôt les « normes techniques » qui ont été défiées par le biais d'une attaque en brèche du quantitativisme alors prévalent. Ce faisant, l'on peut considérer l'émergence d'une « école française des usages » comme celle d'une troisième voix entre les scénarios « grand public » et les scénarios « administratifs »<sup>72</sup>, les premiers étant brocardés pour leur caractère excessif et normatif, les seconds mis à l'amende pour la frilosité et l'abstraction des visions proposées :

*« les premiers tendent à le réduire à une sorte de démonstration des modes d'emploi actuels ou supposés des services des machines ; pour les seconds, l'usage n'est le plus souvent traité que comme variable accessoire, voire comme la résultante de la confrontation entre les stratégies de l'offre et les tendances socio-économiques ou politiques. »* (Mercier & Toussaint, 1994)

En se plaçant en cet endroit, l'« école française des usages » a consolidé l'essence dynamique du concept, comme étant avant tout « *l'aboutissement d'un processus de négociation et de convergence entre un dispositif technique, des réseaux et des groupes sociaux, des imaginaires et des formes spécifiques d'appropriation.* » (Bajolet, 2005 p. 51). C'est cette posture épistémologique qui a commandé l'équipement en outils d'investigation nouveaux, c'est-à-dire en outils d'investigation inusités jusqu'alors dans les études dont

---

<sup>71</sup> Cf. partie suivante

<sup>72</sup> « Les scénarios « grand public », optimistes ou catastrophistes, sont essentiellement fondés sur la concrétisation supposée des virtualités connues de l'innovation technique à travers des produits et des services de grande diffusion : la médiation technique est omniprésente, et les usages des services ou machines sont conformes à leur fonctionnalité supposée. Les scénarios « scientifiques » ou « administratifs » résultent en général d'une démarche prospective qui privilégie les tendances (techniques, économiques, politiques, démographiques, éventuellement socio-culturelles) repérables ou, du moins, déclinables en fonction de leur degré de probabilité. Ces tendances sont modulées et croisées pour obtenir des scénarios tendanciels, plausibles, « scénarios-cadres » en quelque sorte, déclinant une ou plusieurs voies moyennes en termes macro-économiques et macro-sociologiques. » (Mercier & Toussaint, 1994)



l'objet était pour partie constitué par les TIC. Quel que soit le niveau d'étude privilégié<sup>73</sup>, les chercheurs, armés d'un cadre théorique commun, étaient également soudés par un même principe méthodologique : la revendication d'une approche qui « *consiste à observer les pratiques réelles, de conception, de diffusion, d'usage, mais aussi de construction des représentations et du sens de la technique, au travers d'enquêtes de terrain sociologiques, microsociologiques ou ethnographiques.* » (Bajolet, 2005 p. 29)

C'est donc à travers le dépassement d'un cadre quantitativiste dont la dénotation politique constitue une gêne<sup>74</sup>, que peut se lire l'acte de transgression originel de l'« école française des usages ». L'« usage », *déquantifié* par l'entremise de méthodes compréhensives et impliquantes<sup>75</sup>, est en réalité le catalyseur qui fait entrer en déviance un nombre croissant de chercheurs résolus à témoigner autrement :

*« L'usage est un phénomène complexe qui se traduit par l'action d'une série de médiations enchevêtrées entre les acteurs humains et les dispositifs techniques. L'observation des usages des objets techniques, c'est-à-dire de ce que les gens font effectivement avec ces objets et ces dispositifs, peut donc constituer une entrée méthodologique pertinente pour saisir l'action de la technique dans la société. La description précise, l'analyse et la compréhension nuancée des phénomènes d'usage et d'appropriation des objets et dispositifs techniques permettent de saisir avec plus de finesse*

<sup>73</sup> Pierre-Alain Mercier (1993) distingue les études qui se placent durant la genèse de l'innovation technique, durant l'inscription de la technique dans des pratiques préexistantes et au moment de la différenciation sociale des formes d'usage

<sup>74</sup> « Aussi en est-on venu à considérer dans les études de prospective : 1. Les rapports qu'une rationalité entretient avec un imaginaire (qui est dans le discours l'indice de son lieu de production) ; 2. La différence entre les tâtonnements, ruses pragmatiques et tactiques successives qui jalonnent l'investigation pratique et, d'autre part, les représentations stratégiques qui sont offertes aux destinataires comme le produit final de ces opérations. On constate, dans les discours, le retour subreptice d'une rhétorique métaphorisant les « champs propres » de l'analyse scientifique, et, dans les bureaux d'études, une distance croissante des pratiques effectives et quotidiennes (qui sont de l'ordre de l'art culinaire) par rapport aux écritures en « scénarios » qui jalonnent de tableaux utopiques le murmure des manières de faire en chaque laboratoire : d'une part, des mixtes de science et de fiction ; d'autre part, la disparité entre les spectacles de stratégies globales et l'opaque réalité des pratiques locales. On est donc amené à s'interroger sur les « dessous » de l'activité scientifique, et à se demander si elle ne fonctionne pas à la manière d'un collage qui juxtapose, mais articule de moins en moins les ambitions théoriques affichées par le discours et la persistance têtue, rémanente, des ruses millénaires dans le travail quotidien des bureaux et des labos. En tout cas, cette structure clivée, observable en tant d'administrations ou d'entreprises, oblige à repenser toutes ces tactiques jusqu'ici trop déniées par l'épistémologie de la science. Le problème ne concerne pas seulement les procès effectifs de la production. Il met en cause sous une forme différente, le statut de l'individu dans les systèmes techniques, puisque l'investissement du sujet diminue à la mesure de leur expansion technocratique. » (De Certeau, 1990 p. LII)

<sup>75</sup> « Pendant quelques années, la quasi-totalité des sociologues des usages des NTIC se reconnurent dans ce type d'approche. Délaissant les approches quantitatives, ils s'appliquèrent à repérer les manières de faire, prendre le temps d'observer, d'écouter et de revenir sans cesse sur les formes d'usage afin de les modéliser. Leur sociologie est donc qualitative et nécessite dans tous les cas une forte implication des chercheurs. Il leur faut en effet intervenir pour constater, intervenir pour vérifier, intervenir pour comprendre. Car à partir du moment où on parle de "braconnages", de "détours" et de "pratiques de résistance", il faut s'attendre à ne pas pouvoir les lister d'avance. Et si ces usages se rapportent de surcroît à des techniques nouvelles, il faudra par définition s'immiscer pour observer. C'est pour cette raison que les méthodes employées par les sociologues des usages sont toutes intervenantes : il s'agit d'observer en situation, d'écouter attentivement, d'entretenir longuement. » (Jaureguiberry, 2008 p. 33)

*la complexité et les subtilités de la détermination du phénomène technique dans notre vie quotidienne. » (Breton & Proulx, 2002 p. 254)*

## ***B - L'apprentissage social : l'établissement d'un collège invisible***

Pour Pierre Chambat, l'usage est une « *notion carrefour* », « *occasion de confrontations entre les disciplines qui se partagent le champ de la communication* » (Chambat, 1994 p. 263). Ces confrontations sont donc caractéristiques d'un champ de recherche profondément marqué par la variété des disciplines qui ont concouru à son essor. Lorsqu'elle revient sur la genèse de l'« école française des usages », Josiane Jouët (2000) n'oublie pas de souligner le peu d'influence qu'ont eu les approches culturalistes anglo-saxonnes ainsi que la sociologie de la réception (Hoggart, 1972 ; Hall, 1973 ; Silverstone & Hirsch, 1992) sur l'émergence du mouvement, et ce, malgré les accointances théoriques évidentes (Forest, 2003). Ce sont sur les sociologies qui suivent les événements de 1968 et qui s'intéressent particulièrement au changement social, à la montée de l'individualisme et à l'autonomisation des pratiques, que l'« école française des usages » se fonde<sup>76</sup>. Sociologues de la famille, du travail, des modes de vie et mêmes politologues sont donc les précurseurs d'un champ de recherche qui sera investi, dès la fin des années 80, par d'autres courants : sociologie de la diffusion (Rogers, Everett M., 1983 ; Boullier, 1989 ; Boczkowski, 2004 ; Cormerais, 2004), sociologie de l'innovation (Akrich & Boullier, 1991 ; Akrich, Callon & Latour, 2006), ethnométhodologie (De Fornel, 1992 ; Licoppe, 2002), histoire des techniques (Flichy, 2003), science de l'information et de la communication (Miège, 1997 ; Jeanneret, 2000 ; Le Marec, 2001 ; 2004), approches socio-politiques<sup>77</sup> (Gras, Joerges & Scardigli, 1992 ; Vedel, 1994 ; Vitalis, 1994). Ainsi, l'interdisciplinarité de la mal-nommée « sociologie des usages » tire sa justification du « *travail de recherche au complet* » qui

---

<sup>76</sup> « Les années 70 constituaient la fin de la longue période de l'après-guerre, pendant laquelle la priorité incontestée allait à la croissance économique, elle-même assurée par la technicisation progressive de tous les domaines de l'activité industrielle et sociale. [...] Et de fait, cette période voyait se développer un rapport de force très inégal entre les grands acteurs qui portaient cette priorité [...]. Mais pourquoi les premières observations semblaient-elles confirmer le bien-fondé de pareils modèles ? Parce que les sciences sociales s'attachaient à décrire des changements choisis parmi les dimensions du mode de vie que l'on jugeait, à l'époque, les plus importantes [...]. Les années 80 et 90 voient une remise en cause progressive de ce consensus. [...] Le chercheur s'applique désormais à découvrir le sens que chaque micro-acteur social entend donner à sa vie, ce qui se traduit par des recherches sur les comportements de refus ou de dysfonctionnement, les contournements d'usage imposés et les détournements de sens ; ou, plus largement, sur la sociologie de l'appropriation sociale de la technique dans la vie quotidienne, mais aussi sur l'action collective autour de la mise en place de telle ou telle technique à l'échelon du quartier ou de l'atelier. (...) C'est un passage du "produit" – bien ou service qui intègre la nouvelle technologie – à la personne, à la fois consommateur, travailleur, habitant d'une cité. » (Scardigli, Victor, 1994 p. 309-310)

<sup>77</sup> « Afin d'éviter les impasses d'une analyse centrée exclusivement sur le pouvoir et les ruses de l'individu-consommateur, une approche socio-politique des usages entend contextualiser ces derniers et les replacer à l'intérieur de la société actuelle. Il s'agit, en d'autres termes, de reconnaître le pouvoir de l'utilisateur, mais un pouvoir contraint et fortement limité par le pouvoir dominant de la production. » (introduction de Vitalis, 1994 p. 9)

*s'effectue parce qu' « autour d'un instrument, d'un objet ou d'un terrain, la mobilisation de ressources de plusieurs disciplines s'impose parfois. » (Vinck, 2007 p. 84)*

Comme nous l'avons préalablement démontré, c'est l' « usage » des TIC, ou plutôt sa problématisation<sup>78</sup>, qui articule le collectif de chercheurs qui collaborent, se rencontrent, discutent au profit d'une certaine circularité des savoirs : l'emprunt de méthodes, d'outils et de concepts à d'autres disciplines que la sienne est monnaie courante (Vinck, 2000) et sert plus la réflexion sur l'objet qu'il ne consolide les frontières disciplinaires. La sociologie des usages est, dès le début des années 80, marquée par l' « *effervescence de bricolage intellectuel et d'artisanat conceptuel* » (Jouët, 2000 p. 493).

Cette socialisation de l'activité déviante est stimulée par deux phénomènes concomitants (Jouët, 2000). D'une part, la recherche a pu bénéficier du soutien appuyé d'un Etat en situation de quasi monopole sur le plan industriel. Celui-ci s'effectuait soit par l'intervention de grands groupes industriels, alors nationalisés, soit directement, par l'entremise de l'administration<sup>79</sup>. Parmi les espaces de recherches qui se sont insérés entre la livraison des commandes passées, Josiane Jouët souligne le rôle initiateur de la Direction de la Recherche Prospective de l'Institut National de l'Audiovisuel (INA), l'activité d'émulation du CESTA (Centre d'Etudes des Systèmes et des Technologies Avancées), et accorde la palme de la stimulation des activités de recherche à la Direction Générale de Télécommunications (DGT) et au Centre National d'Etudes des Télécommunications (CNET), tous deux producteurs de nombreux appels d'offre, parfois en collaboration avec le Ministère de la Recherche. La communauté de recherche qui gravite autour des problématiques d' « usage » est alors constituée de « *sociologues atypiques (universitaires, CNRS ou indépendants), quelques chercheurs en communication comme ceux du GRESEC et, d'autre part, des membres du Service de la prospective de la DGT et du Département des usages sociaux des télécommunications du CNET.* » (Jouët, 2000 p. 492-493)

D'autre part, ces chercheurs jouissent d'une grande liberté d'action leur permettant, le cas échéant, de snober les *a priori* quantitativistes figurant dans les cahiers des charges des commandes passées :

---

<sup>78</sup> « Cette dérive émergente vers l'empirisme témoigne d'une cristallisation sur l'objet qui l'emporte sur la problématique et l'usage instrumental des machines à communiquer devient parfois le cœur de l'observation, en postulant implicitement que l'usage peut se suffire à lui-même, existe en soi et n'est pas le fruit d'une construction sociale. » (Jouët, 2000 p. 513)

<sup>79</sup> « Dans les années 60, les grands groupes industriels se dotent d'importants centres de recherche, qui sont des corps étrangers mal intégrés à l'ensemble de l'activité produite. Ce mouvement s'accroît avec les nouvelles technologies qui impliquent plus de transversalité. Dans les années 1980, l'action croisée des politiques de recherche et des politiques industrielles inscrit la recherche scientifique dans le jeu des échanges économiques et dans le registre de l'utilité sociale (emploi, compétitivité, utilisation efficace de l'argent public). Des groupes industriels en viennent à occuper une place stratégique dans les contrats de recherche publique et deviennent le passage obligé des industriels du secteur. » (Vinck, 2007 p. 99)

*« A cette époque, les commanditaires ont judicieusement distingué les études de marketing, réalisées par des bureaux conseils, des recherches sociologiques dont l'objectif n'était pas tant de fournir des clés pour l'action que de comprendre les réactions du corps social face à l'arrivée des nouveaux objets de communication. Les chercheurs ont pu bénéficier de l'autonomie scientifique requise pour la conception des enquêtes, pour l'analyse des résultats et les publications, comme disposer du temps de maturation nécessaire à la recherche. Ces bons augures ont favorisé une grande fécondité des échanges dans le petit réseau d'une douzaine de chercheurs travaillant alors sur les usages sociaux des TIC. » (Jouët, 2000 p. 493)*

L'espace de recherche obéit ainsi, en tendance, aux règles du « régime de recherche scientifique et technique transitaire », tel que pensé par Pestre (1997) et Shinn (2000) et dont nous empruntons la définition à Dominique Vinck (Vinck, 2007) :

*« Les chercheurs y oscillent entre deux critères de sélection des thèmes de recherche et deux marchés de diffusion des résultats : la recherche fondamentale (réfèrent universitaire) et la sphère socio-économique. Ils passent de l'un à l'autre en fonction de leurs besoins. En dernière instance, leurs préférences, en termes de contenu de recherche, de public et de réputation, portent sur le long terme, la recherche désintéressée et l'échange avec leurs pairs. Toutefois, une partie de l'activité de recherche et de la trajectoire professionnelle se joue à la marge des institutions de la discipline, se rapprochant soit d'autres disciplines, soit de l'ingénierie ou de l'action (managériale, politique, médicale...). Ils circulent dans ces autres domaines en fonction de leurs besoins en termes de techniques, de données, de concepts et d'alliance. Ils opèrent leurs choix, selon les cas, en fonction de critères de leur discipline d'origine ou de la discipline d'alliance. De façons similaires, la diffusion de leurs travaux se fait tantôt dans les revues académiques disciplinaires, tantôt dans les milieux socio-économiques. » (p. 85)*

L'inscription dans ce régime de savoir permet à l'approche par l'« usage » et à ses défenseurs de bénéficier d'un régime de tolérance. S'ils sont étiquetés comme déviants, la position d'agents doubles qu'ils occupent – alternativement dans et hors l'institution, offre aux transgresseurs la possibilité d'assumer leur rôle d'outsiders sans pour autant être victimes d'une stigmatisation violente. Cette posture habilite donc un usage social de l'« usage » d'une douce indocilité.

## ***C - La désignation publique : la production scientifique comme lieu d'organisation***

Bien que l'école française des usages relève plus du « collège invisible<sup>80</sup> » que d'une institution formalisée et unie, nous avons souhaité rechercher des traces des formes d'organisation de ce champ de recherche nous permettant d'aborder la question de la désignation publique de cette déviance en conditionnant la possibilité de celle-ci à l'existence d'un travail d'organisation et de mécanismes de coordination effectifs. Ainsi, certains points abordés dans la partie précédente renseignent déjà sur les formes d'organisation mises en place par l'école des usages. Ainsi, le consensus dogmatique sur l'« usage » comme construit social, l'intérêt porté aux TIC, les méthodologies d'investigation déployées, sont autant d'indices de présence de formes d'organisation, sinon de coordination. Néanmoins, si le rôle de l'Etat dans la structuration de la recherche nous aide à comprendre la genèse de l'école française des usages et la logique « top-down » alors prévalantes, il nous faut renseigner davantage la mécanique de coordination à l'œuvre. La question à laquelle nous avons voulu répondre est celle du lieu à partir duquel on puisse déceler des indices de « *la structure d'autorité, [des] règles et [des] procédures, [de] la formalisation des objectif et des tâches, [de] la standardisation des compétences, des tâches et/ou des résultats, [des] systèmes de communication et d'ajustement.* » (Vinck, 2007 p. 92) Dès lors, la qualification de l'école française des usages comme « collège invisible » montre toute son utilité heuristique ici. En effet, les collèges invisibles<sup>81</sup>, véritable lieux d'intensification des liens entre les membres qui les composent<sup>82</sup>, ont une caractéristique typique observée grâce aux études bibliométriques (Crane, 1969 ; Griffith & Mullins, 1980) : un degré relatif de prédictibilité des comportements de ses membres observable à travers l'étude du partage d'information et des formes de collaboration. Entre autres comportements étudiés, on retiendra notamment le développement de liens faibles en dehors du réseau de prédilection (Granovetter, 1973), un des phénomènes observés est la croissance exponentielle des publications du collège invisible (Price, 1986).

Sans nous livrer à une étude bibliométrique ou scientométrique de la production de ce collège invisible et n'ayant pas eu l'opportunité d'interviewer les principaux tenants de

---

<sup>80</sup> Le terme collège invisible vient du XVII<sup>ème</sup> siècle et revoie à la fondation de la royal Society of London. Les membres de celle-ci, pour la plupart mathématiciens, n'appartenaient pas à une institution particulière. Ils utilisaient le terme collège invisible pour parler d'eux-mêmes en raison de leur proximité géographique et de la régularité des réunions fondées sur une communauté d'intérêts scientifiques. (Price, 1971 ; Lievrouw, 1990)

<sup>81</sup> Pour une réflexion approfondie, voir (Zuccala, 2006)

<sup>82</sup> « For each group there exists a sort of commuting circuit of institutions, research centers, and summer schools giving them an opportunity to meet piecemeal, so that over an interval of a few years everybody who is anybody has worked with everybody else in the same category. » (Price, 1986 p. 76)

l'approche par l'usage – un travail qui sans doute pourrait constituer un riche matériau de réflexion, nous nous sommes limités à l'identification des lieux de publication de ce courant de recherche. Puisque celui-ci répond, ou du moins s'en justifie, aux « *normes éthiques* » de la science (Merton, 1973), ses productions scientifiques sont soumises à des procédures de contrôle et d'évaluation systématiques des résultats. Ce jugement par les pairs est un moyen d'organisation et de contrôle de la cohésion du groupe et des conditions d'entrée et de sortie de celui-ci (cf. partie II). Ainsi, c'est par l'examen de la structure du champ littéraire que nous avons identifié les formes de coordination à l'œuvre dans l'école française des usages.

Tout d'abord, c'est autour d'une revue, lancée en 1983 et vouée à accompagner le développement des sciences sociales au Centre National d'Etudes des Télécommunications (CNET), que s'est structuré le champ (Flichy, 2008) : la revue *Réseaux* fondée par Paul Beaud et Patrice Flichy<sup>83</sup>. Celle-ci a, dès son lancement, été envisagée comme « *un outil permettant de structurer un champ de recherche en cours de constitution* » (Flichy & Quéré, 2000 p. 10). Toujours en activité (6 numéros par an ; 160<sup>ème</sup> numéro au printemps 2010), la revue a accueilli de nombreux travaux d'investigation et d'analyse de chercheurs provenant d'horizons disciplinaires différents mais tous attachés à la question de l'usage des TIC. Elle constituait un lieu d'échanges, de discussions, de normalisation et de mise en visibilité des acteurs du courant et de la conformité de leurs travaux. Notons, à cet égard, que de nombreux articles émanent de rapports produits à destination de commanditaires et dont la diffusion était cependant rendue possible par le biais de la proximité entre chercheurs de cette communauté de recherche. Certains de ces rapports ont même fait l'objet d'un travail éditorial classique, comme le rapport Musso pour la DATAR (Musso, 1994).

Aussi, la fréquence d'occurrence de certains ouvrages dans les bibliographies de la littérature grise témoigne du rôle de credo joués par ceux-ci. On pense ici, sans prétention d'exhaustivité, d'abord à Michel de Certeau et son *Invention au quotidien* (De Certeau, 1990) dont Serge Proulx avait relevé l'influence paradigmatique (Proulx, 1983), au *magnétoscope au quotidien : un demi-pouce de liberté* de Baboulin, Gaudin et Mallein (1983) ou encore à l'essai sur les machines à communiquer de Jaques Perriault, *la logique de l'usage* (Perriault, 1989). Plus récemment, on peut citer sans risque l'*histoire de la communication moderne et l'innovation technique* de Patrice Flichy (1991 ; 2003), la *sociologie des techniques de la vie quotidienne* édité par Gras, Joerges et Scardigli (1992), le

---

<sup>83</sup> Le rôle de structuration de la revue est ici souligné bien que d'autres revues aient également hébergé des travaux importants. On pense notamment à certaines revues du champ disciplinaire des sciences de l'information et de la communication (*Hermès* fondée par Dominique Wolton ; *Quaderni* fondée par Lucien Sfez ; *Communication et langage* ; *Technologies de l'information et société*) ou d'autres revues plus généralistes comme la revue *Esprit* (notamment le n° 186 avec des contributions de Chantal de Gournay, Pierre Chambat et Yves Toussaint).

*dictionnaire critique de la communication* mis en œuvre par Lucien Sfez (Sfez, 1993) et *l'explosion de la communication* de Breton et Proulx (2002) comme des productions scientifiques et littéraires structurantes de l'école française des usages.

Enfin, les actes de certains colloques ont attiré notre attention par leur présence répétée dans la littérature examinée. Il s'agit du colloque « Machines à communiquer » qui a eu lieu au parc de La Villette en 1991 et donné lieu à la publication d'un ouvrage dirigé par Pierre Chambat (1992), le cinquantenaire du CNET en 1995 et le Colloque International « *Penser les usages/ (Télé)communications 97* » qui a eu lieu à Arcachon en 1997 (Collectif, 1997).

### ***D - La perpétuation de pratiques et savoir-faire : l'espace national comme ancrage***

Le succès des études d'usages trouve confirmation dans la multiplication des appels d'offre émanant d'une gamme plus large d'institutions :

*« [...] nous assistons, à l'aube du nouveau siècle, à une véritable frénésie du côté des appels d'offre en matière d'études d'usage. Alors qu'elles ont été longtemps considérées comme les parents pauvres de la recherche sur les TIC (les études valorisées étant alors celles concernant les impacts des TIC sur les industries culturelles et l'évaluation sociopolitique des stratégies des acteurs publics et industriels), voilà qu'aujourd'hui nous assistons à une véritable « mode des études d'usage » tous azimuts, cette mode comportant le risque énorme de sombrer sous un déluge de rapports de recherches empiriques très pointues et extrêmement parcellaires et n'offrant plus de problématisation adéquates ou de cadre d'analyse s'appuyant véritablement sur les acquis de recherches passées. Nous éprouvons un malaise vis-à-vis de cette réduction des problématiques concernant les usages à des questions et objectifs de marketing. » (Breton & Proulx, 2002 p. 275)*

Par effet d'apprentissage constaté plus haut, le « collège invisible » s'est constitué comme réseau « *forum*<sup>84</sup> » (Vinck, 1992) compact sans dissension majeure quant à la manière d'envisager l'« usage ». Ainsi, cette perpétuation de pratiques et savoir-faire s'est

---

<sup>84</sup> « C'est une « structure sociale dans laquelle les scientifiques échangent des idées et des résultats, conçoivent des projets (bilatéraux ou collectifs), conviennent de codes de conduite. Le « forum » repose sur des échanges « classiques » entre équipes : séminaires et colloques. Il permet de structurer une communauté scientifique autour de questions de recherche, d'objets d'études ou de méthodologies. Il se rencontre là où il s'agit d'organiser de petites communautés spécialisées et d'explorer des problèmes à la frontière des disciplines. Il s'accommode éventuellement de l'absence de laboratoire. » (Vinck, 2007 p. 114)

irradiée du laboratoire à la communauté scientifique, de la communauté scientifique aux conseils de recherche, des conseils de recherches à la société. L'école française des usages a ainsi réussi à ce que cet ancrage géographique (la France) dépasse son enracinement scientifique. La publicisation des études d'usage ainsi que la sollicitude grandissante d'institutions variées pour celles-ci s'inscrivent dans une logique politique de décentrement des prises de décisions concernant le développement et la diffusion des TIC. Cette forme de gouvernance revendiquée, incarnée par la vigueur des formes de dialogues entre science et société ou entre technologie et société, marque d'une certaine manière l'aboutissement sociétal d'une lutte de légitimité des études d'usages.

Cependant, le succès de cette diffusion au-delà des cercles savants se comprend également par l'intérêt grandissant des acteurs économiques du secteur des télécommunications ; et cette attention n'est pas sans incidence. D'abord, elle altère subrepticement la définition de l'usager qui dérive d'une appréhension comme citoyen, passe par celle de client pour devenir enfin consommateur<sup>85</sup>. D'autre part, cet intérêt se traduit de deux manières (Jaureguiberry, 2008). Les opérateurs de télécommunications peuvent agir dans une optique d'adaptation de leurs messages publicitaires aux usages qui ont le plus de succès. Ils s'appuient alors sur les résultats d'enquêtes quantitatives connues sous le nom d'Usages et Attitudes (U&A). D'autre part, les opérateurs peuvent faire appel à des sociologues qualitatifs pour « *intégrer des pratiques d'“usages porteurs” dans la “conception permanente” des objets techniques.* » (Jaureguiberry, 2008 p. 38). Ils se rapprochent en cela plus de la notion d'« usage » telle que développée par l'école française. Ces deux cas d'utilisation marchande du concept vont avoir un impact important sur la communauté de chercheurs travaillant sur l'« usage ». L'une des conséquences est l'éclatement des objets de recherche des chercheurs soumis aux impératifs de la recherche contractuelle. En effet, la multiplication des TIC décentre l'intérêt pour l'usage et oriente les recherches vers les spécificités de l'objet ou de la technologie en développement sans pour autant que des ponts soient jetés entre chacun des travaux :

*« Ce large éventail permet une accumulation de données mais il est aussi source d'émiettement car les nouvelles études ne se fondent pas toujours sur une capitalisation des travaux antérieurs, « redécouvrent » des acquis et n'ouvrent pas nécessairement de nouvelles pistes. La démarche comparative, pourtant si riche pour le développement des problématiques en sciences sociales, n'est pas nécessairement empruntée et chaque objet*

---

<sup>85</sup> « Considéré comme “un citoyen plus ou moins prioritaire pour obtenir une connexion” jusqu'au début des années 1970, puis comme “clients” dans les années 1980, l'usager devient dans les années 1990 “un consommateur exigeant dont les besoins et les attentes font l'objet d'une attention particulière” (Carré & Panico 1997). » (Jaureguiberry, 2008 p. 38)



*d'étude paraît comme un dispositif radicalement nouveau, alors que des fils peuvent être tissés entre les usages des diverses technologies d'autant que la continuité et la reproduction des pratiques font partie des acquis du courant.* » (Jouët, 2000 p. 513)

L'autre conséquence, liée, concerne l'attitude des chercheurs à l'endroit de ce mouvement de mode. Ceux-ci, confrontés à la répercussion de la pression du marché qui s'exerce sur l'ensemble des opérateurs, et plus précisément sur les anciens monopoles d'Etat subissant l'ouverture à la concurrence de leur secteur, n'ont au fond que trois alternatives (Jouët, 2000) : soit travailler dans l'ombre d'une recherche sous contrat avec des contraintes matérielles fortes, soit se soumettre à l'exigence de productions d'études empiriques sans profondeur théorique soit enfin, allier réalisation d'études de terrain et productions scientifiques, ce qui, cela va sans dire, réclame un investissement supérieur et des qualités d'équilibristes certaines.

Cette rançon du succès des études d'usage a également donné licence à certains chercheurs pour interroger l'école française des usages dans ses apports théoriques. La dérive empiriciste a permis de pointer du doigt le désintérêt majoritaire des études d'usage pour la conception des technologies qu'elles étudiaient, ce dans le contexte d'une théorie de l'acteur-réseau en vogue<sup>86</sup>. De manière imbriquée, est remise en question la distinction entre *technique* et *social* qui laisse impensée la question des choix techniques effectués. Quant aux bienfaits de l'interdisciplinarité, ils sont relativisés par l'autonomisation du traitement de l'« usage » au sein de certaines disciplines, notamment les sciences de l'information et de la communication et la psychologie, qui laissent dans l'angle mort les questions attenantes aux processus sociaux de formation des usages : l'usage s'en trouve réduit dans une définition locale et contextuelle sans que celui-ci « pourtant pris dans des structures qui limitent constamment ses capacités de résistance, de bricolage ou de détournement » ne fasse l'objet d'un questionnement sur ces qualités d'agent, « *chose qu'un enfermement sur l'usager pris comme une monade ne permet pas.* » (Jaureguiberry, 2008 p. 40)

La centralité accordée au discours de l'usager en contexte d'utilisation relègue paradoxalement celui-ci au rang duquel les sociologues désiraient l'extirper : « *en bout de chaîne, puisque il ne produit plus rien que du discours* » (Le Marec, 2001). L'auteure milite, en conséquence, pour une mise en réflexivité constante du chercheur afin que celui-ci se

---

<sup>86</sup> Notons qu'à l'exception des travaux de Madeleine Akrich (Akrich, 1987 ; 1989 ; 1993), les chercheurs de l'ANT ont souvent limité leur champ d'investigation à l'étape de la conception, même si le cadre conceptuel et les principes de l'ANT prône de suivre les innovations sans limitations à priori. Dans le champ plus large des « sciences studies », l'extension de l'investigation jusqu'à l'utilisateur s'est peu à peu affirmée à partir des années 2000 (voir (Mackay, Carne, Beynon-Davies & Tudhope, 2000 ; Oudshoorn, N. & Pinch, 2003 ; Oudshoorn, Nelly, Rommes & Stienstra, 2004)

dégage des risques de « prédétermination de phénomène » confortant un modèle linéaire de la conception et de l'usage.

## II - L'usage, objet d'une pratique pythique

---

Pour aborder l'analyse de ce que nous avons identifié comme une nouvelle entrée en déviance de l'« usage », nous avons, une nouvelle fois, pu tirer profit de l'environnement au sein duquel nous avons évolué en tant que doctorant. Tout d'abord, du fait de notre hébergement par le CEA-LETI, nous avons tissé des relations tant professionnelles qu'amicales avec la figure idoine de cette entrée en déviance : Philippe Mallein, alors conseiller scientifique auprès du directeur du CEA-LETI. Par ailleurs, c'est au sein des instances de socialisation académique (colloque, séminaire, réunion de travail, etc.) que nous avons pu sentir les tensions cristallisées autour de Mallein et des activités de ses équipes (cf. chapitre précédent). Ces deux éléments ont donc fondé notre intuition à mener cette analyse. Dans cette partie, nous souhaitons examiner la manière dont la méthode CAUTIC™ (Conception Assistée par l'Usage pour les Technologies, l'Innovation et le Changement) représente une forme symptomatique de déviance de l'utilisation de la notion d'« usage ».

Nous avons qualifié cette forme d'usage de *pythique* en référence au mythe attaché au sanctuaire de Delphes. Celui-ci aurait été fondé par le Dieu Apollon qui terrassa le serpent gardien du sanctuaire, « Python » et y établit un oracle destiné à guider et conseiller les hommes. La parole de cette divinité est ainsi transmise aux hommes par l'intermédiaire de la Pythie. Celle-ci entre en correspondance avec l'oracle selon un rite bien ordonné durant lequel plusieurs opérations de traduction ont lieu : un homme produit une question traduite par deux prêtres et leurs assistants à la pythie dont la parole est, après consultation de l'oracle, retraduite par les prêtres pour être compréhensible pour l'homme consultant. Au départ jeune fille vierge et inculte choisie parmi les femmes du voisinage, l'agression de l'une d'elle a fait porter le choix sur des femmes de plus de cinquante ans, issues de familles honnêtes et respectables et ayant mené une vie irréprochable. Ainsi, la Pythie tenait fonction de prophète (étymologiquement « celle qui parle à la place de dieu »). Figure institutionnelle, rattachée à un lieu précis, la Pythie répond aux consultations des hommes et leur donne des indices sur leur destinée. Se servir de la métaphore pythique et oraculaire nous permet, dans un premier temps, de jauger le changement qui s'opère entre l'« usage », objet de *poiétique* et cette forme de mobilisation de l'« usage » : le concept est intégré dans une économie de consultance où il s'agit de prévoir et de communiquer sur le destin social d'innovations en conception. La méthode CAUTIC™, à l'instar de la Pythie, sert d'instrument d'investigation et d'élicitation, instrument légitime par la sagesse de sa construction, la rigueur de son emploi et les compétences des traducteurs. Le recours à cette

métaphore nous servira également à la mise en évidence des caractères discriminant la troisième forme d'usage social de l'« usage » de la forme pythique, les deux formes s'inscrivant dans une logique oraculaire marquée.

Le plan de ce chapitre est calqué sur celui du précédent. Dans un premier temps, nous nous attacherons à identifier la transgression normative que constitue la méthode dans sa manière de mobiliser l'« usage ». Pour effectuer cette opération, la partie débutera par un descriptif de la méthode et de ses outils. Ensuite, nous prendrons appui sur le parcours biographique de Philippe Mallein pour comprendre la dynamique d'apprentissage social qui a entouré la méthode. Seront ainsi abordées les questions de la nature et de la justification de l'interdisciplinarité à l'œuvre et celle du régime scientifique dans lequel s'inscrit la méthode. En troisième lieu, nous nous intéresserons aux formes de coordination et de mobilisation de ressources générées et appelées par le déploiement de cette méthode avant de conclure par la description de l'émergence d'une relève de jeunes chercheurs implantés dans le périmètre de diffusion locale de la méthode.

## ***A - Le passage à l'acte déviant : le pas tournant de la méthode CAUTIC™***

En 1999, le CNRS attribue à Philippe Mallein, ingénieur de recherche dans l'institution officiant à la Maison des Sciences de l'Homme de Grenoble, un Cristal<sup>87</sup> qui vient récompenser la conception de la méthode CAUTIC™. Il eut été aisé de lire dans cette distinction une forme d'exercice de contrôle social d'une institution à l'égard de ses membres (Ihl, 2007) et partant, la reconnaissance d'une certaine exemplarité chez Philippe Mallein. Cependant, et bien que nous n'ayons pas effectué de travail approfondi sur les conditions de remise de cette récompense et de ses conséquences sur le déroulement de carrière du chercheur, l'évocation de cette méthode dans les cercles académiques déclenche invariablement des réactions teintées d'irritation, de mépris voire d'ignorance<sup>88</sup>. Afin de mieux appréhender la déviance attachée à l'usage de cette méthode, nous commencerons notre exposé par une description à grands traits de CAUTIC™<sup>89</sup>.

Comme son acronyme l'atteste (Conception Assistée par l'Usage pour les Technologies, l'Innovation et le Changement), la méthode CAUTIC™ est une forme d'analyse de l'« usage » clairement mobilisée au service d'activités de conception, valorisée commercialement en 1999 par la société Ad Valor<sup>90</sup>. Elle vise à évaluer l'acceptabilité d'un produit ou d'un service par les populations ciblées par les concepteurs. La revendication du caractère novateur de la méthode tient de son intervention durant les phases de conception et non après la réalisation du produit ou du service. L'évaluation et le diagnostic de l'acceptabilité du produit est concomitante du processus de conception afin de pouvoir procéder à des modifications et ajustements avant que toute possibilité d'intervention soit trop coûteuse pour le porteur de projet. Néanmoins, l'utilisation de la méthode est également préconisée a posteriori du lancement du produit/service, afin de pouvoir améliorer une version ultérieure de celui-ci.

---

<sup>87</sup> Le Cristal du CNRS, créé en 1992, distingue chaque année des ingénieurs, des techniciens et des administratifs. Il récompense celles et ceux qui, par leur créativité, leur maîtrise technique et leur sens de l'innovation, contribuent aux côtés des chercheurs à l'avancée des savoirs et à l'excellence de la recherche française (source : <http://www.cnrs.fr/fr>)

<sup>88</sup> Cette attitude est particulièrement aisée à identifier dans la littérature. L'une des tournures les plus radicales consiste en une forme particulière d'ostracisme : il s'agit de ne jamais citer les travaux de Mallein associés à CAUTIC™, ce que Michel Onfray nomme un « autodafé symbolique » lorsqu'il évoque l'ignorance par Platon du courant philosophique hédoniste et de son personnage conceptuel Démocrite (Onfray, 2006)

<sup>89</sup> Ce descriptif succinct de la méthode CAUTIC™ s'appuie sur les sources suivantes (Cautrès & Mallein, 1992 ; Mallein, Forest & Panisset, 1999 ; Heme & Monory, 2001 ; Forest, 2003 ; Mallein, Brun, Cros & Favier, 2004), la page wikipedia de Philippe Mallein ([http://fr.wikipedia.org/wiki/Philippe\\_Mallein](http://fr.wikipedia.org/wiki/Philippe_Mallein)), ainsi que sur une formation que nous avons personnellement suivie en mars 2009, assurée en partie par Philippe Mallein et Céline Verchère.

<sup>90</sup> SARL au capital de 20 000 euros, toujours en activité, Ad Valor a été créée en mai 1999, conformément au projet de loi sur l'innovation, avec le soutien du CNRS et de l'Université Pierre-Mendès-France, à travers la Maison des sciences de l'homme MSH-Alpes de Grenoble. Ad Valor exploite, développe et commercialise la méthode CAUTIC™. La société a pour objectif de mettre au point une gamme de services innovants permettant d'associer l'anticipation de l'usage à la conception et à la réalisation de produit/services nouveaux.

A partir du recours aux entretiens semi-directifs en face-à-face, cette méthode revendique sonder les significations d'usage des utilisateurs potentiels d'une innovation afin de « *définir si le dispositif fait sens dans une logique de réception négociée* » (Forest, 2003). Cette valeur d'usage est considérée comme l'élément clé de l'acceptabilité sociale de l'innovation. Au-delà de l'adaptation des outils aux objectifs des enquêtes auxquelles elle répond, la méthode s'appuie invariablement sur deux instruments pour qualifier l'échantillon traité et ses réactions.

D'une part, elle utilise des profils d'usagers. Ils sont fonction du rapport au changement et à l'innovation de l'individu. Ces profils peuvent être mobilisés pour la constitution de l'échantillonnage ou a posteriori, comme variables discriminantes des populations interviewées. Ces profils archétypaux, au nombre de quatre, découlent d'une segmentation fondée sur une combinaison de quatre variables. Il s'agit d'échelles qui mesurent respectivement le rapport au temps (de la rupture à l'inertie), le rapport à soi (individu sujet ou acteur), le rapport aux autres (ouverture ou fermeture à l'altérité) et le rapport au territoire (implantation dans une zone délimitée ou dans un territoire sans limites). La combinaison de celles-ci débouche sur quatre profils :

- Les passionnés, adeptes du changement.

Leur volonté de dicter les règles, de s'imposer, fait d'eux des leaders d'opinions et des faiseurs de tendances. Ils sont au cœur d'un réseau dense de relations personnelles qu'ils cultivent sans se soucier de l'existence de limites territoriales et en toute autonomie<sup>91</sup>.

- Les pragmatiques du changement.

C'est un profil d'utilitaristes à la recherche de la maximisation de l'efficacité de l'usage du produit/service. Leur prise de risque est maîtrisée et opportuniste car ils appuient leurs actions sur des succès passés.

- Les pragmatiques de la continuité

Ils ont pour quête la continuité et en ce sens, n'acceptent le changement que dans ses formes marginales. Evoluant au sein d'un environnement restreint, ils n'acceptent le changement que lorsqu'il s'impose comme la seule alternative possible.

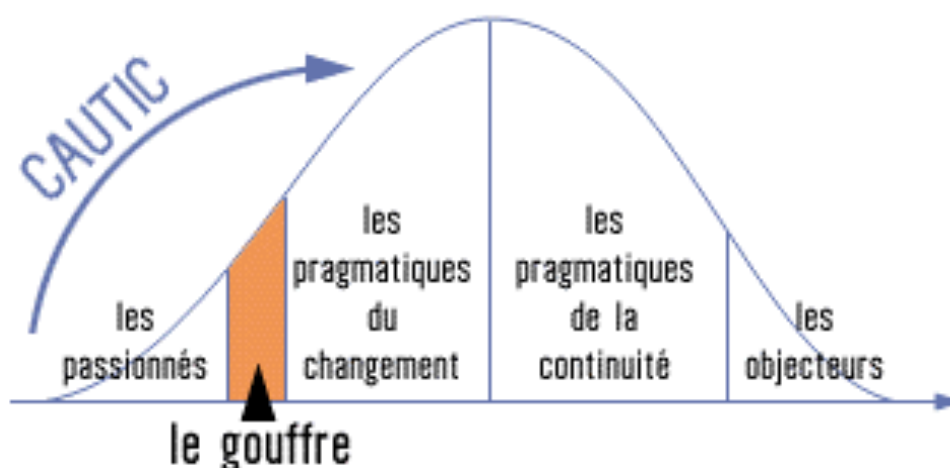
- Les objecteurs au changement

---

<sup>91</sup> L'influence de la théorie de la « communication à double étage » (Lazarsfeld, Berelson & Gaudet, 1944) est ici manifeste.

Conformité et tradition sont le moteur de leurs comportements. Ainsi, le changement est vécu avec angoisse par ces individus qui évoluent dans des univers clos et développent peu de lien social.

Figure 4. Profils d'utilisateurs (Mallein, Forest & Panisset, 1999)



D'autre part, la méthode CAUTIC™ mobilise un guide d'entretien très structuré qui vise à recueillir les « *significations d'usage* » des interviewés. La combinatoire de ces significations constitue le sens de l'usage de l'innovation. La vingtaine de critères utilisés est déclinée en quatre niveaux de significations dans lesquels sont évalués :

- L'assimilation de l'innovation aux savoir-faire techniques familiers de l'utilisateur
- L'intégration de l'innovation au sein des pratiques courantes
- L'appropriation de l'innovation en fonction de l'identité de l'utilisateur
- L'adaptation de l'innovation à l'environnement social et/ou professionnel de l'utilisateur

La phase d'analyse repose sur une validation des critères au regard de deux logiques de conception. La première est une logique de négociation qui prend en compte le sens attribué par l'utilisateur à l'innovation. Elle est opposée à une logique de persuasion, logique d'imposition, par les concepteurs de l'innovation, de sens et de fonctionnalités qui négligent les caractéristiques de l'utilisateur et de son environnement. Le tableau suivant permet de comparer, pour chaque niveau de significations d'usage, les moteurs qui animent ces deux logiques :

Figure 5. Les quatre couples d'opposition conceptuelle de CAUTIC

Une grille d'analyse pour deux rationalités d'usage La nouvelle technologie de l'information et de la communication (NTIC) est confrontée :	
Usage et rationalité de la cohérence socio-technique	Usage et rationalité de la performance techno-sociale
1. aux techniques existantes	
Banalisation En s'accrochant aux techniques existantes la NTIC désigne un objet naturel et ordinaire de la vie quotidienne	Idéalisation En se dégageant des techniques existantes, la NTIC désigne un idéal d'usage et un usager idéal
2. aux pratiques d'information et de communication de l'utilisateur	
Hybridation L'usage de la NTIC se greffe sur les pratiques existantes et permet ainsi le développement à la marge de pratiques nouvelles	Substitution L'usage de la NTIC se substitue aux pratiques existantes et désigne des pratiques radicalement nouvelles
3. à l'identité sociale de l'utilisateur	
Identité active Dans l'usage de la NTIC, l'utilisateur peut agir ou jouer sur son identité sociale	Identité passive Dans l'usage de la NTIC, l'utilisateur est assigné à une identité sociale codifiée
4. à l'évolution de la société	
Evolution sociale L'usage de la NTIC accompagne les grandes tendances de l'évolution sociale en cours. Par cet accompagnement, il influence cette évolution.	Révolution sociale L'usage de la NTIC impose de nouveaux rapports sociaux et de nouvelles formes de lien social
Le producteur de NTIC a donc le choix entre :	
Une logique de négociation entre impératifs techniques et d'usage, exigeant de nombreux aller-retour pendant la conception mais favorisant la diffusion large de la NTIC	Une logique de persuasion facteur de recrutement rapide d'utilisateurs "pionniers" mais comportant des risques de démobilisation ultérieure et d'inadaptation à une diffusion élargie de la NTIC

Chaque critère est alors considéré comme « validé », « validé sous condition » ou « non validé. » Ces deux dernières options engagent le concepteur à des modifications de l'invention pour en optimiser les significations d'usages.

Aussi, la validation de ces critères dépend des « *profils d'utilisateurs* » considérés. Si seuls les passionnés ont des significations d'usage favorables, on peut s'attendre à ce que le cycle de diffusion de l'innovation soit court. Lorsqu'une diffusion large de l'innovation est l'objectif, l'enjeu est le recueil d'un maximum de significations d'usage positives parmi la population des pragmatiques, qui constitue la majorité des publics d'utilisateurs. Cette analyse



est largement inspirée par les études diffusionnistes qui étudient les cycles de diffusion de l'innovation (Rogers, Everett M., 1983) ainsi que par les développements ultérieurs de Moore<sup>92</sup>. On y perçoit également l'influence de la sociologie de l'innovation, dans cette manière de considérer la technique comme ne s'imposant pas d'elle-même, de considérer que des choix sont possibles et qu'il n'y a pas diffusion sans transformation et sans adaptation à des publics divers et variés<sup>93</sup>

Cette courte description de la méthode CAUTIC<sup>TM</sup> nous offre déjà suffisamment d'éléments de compréhension du caractère transgressif de celle-ci. Un écart à la norme qui touche autant le respect des dimensions éthiques que celui des règles méthodologiques. Commençons notre analyse par ces dernières.

L'adoption d'une méthodologie qualitative pour le recueil de l'opinion ne suffit pas à identifier la méthode CAUTIC<sup>TM</sup> comme la fille légitime de l'école française des usages. En effet, CAUTIC<sup>TM</sup> prend plutôt à contre-pied certains fondements théoriques de celle-ci. Tandis que le discernement des deux logiques (« *cohérence sociotechnique* » vs. « *rationalité technosociale* ») participe d'une réflexion au long cours (Mallein & Toussaint, 1975), l'engagement de cette réflexion sur les voies de la formulation de préconisations opérationnelles ne s'est effectué qu'au milieu des années 90<sup>94</sup> (Mallein & Toussaint, 1994). En ce sens, CAUTIC<sup>TM</sup> constitue une forme d'accentuation revendiquée de ce glissement de l'analyse au conseil. Il ne s'agit plus de démontrer la pluralité et la contingence des significations d'usages mais de s'en saisir comme d'un instrument de régulation de l'innovation. Ce changement dans la finalité de l'enquête met en doute la conformité de la méthode aux normes défendues par les premiers tenants de l'« école française des usages » : les normes mertonniennes de la science. D'abord, parce que la méthode, formalisée et

---

<sup>92</sup> Consultant de la Silicon Valley, Geoffrey Moore a développé le travail de Rogers en expliquant les différences entre groupes adoptant l'innovation par leurs motivations (Moore, 1991). Le concept de gouffre (Chasm) vient ainsi caractériser l'écart radical entre les motivations des early adopters (qui correspondent aux passionnés dans CAUTIC<sup>TM</sup>) et celles de l'early majority (les pragmatiques du changement). L'enjeu, pour qu'une innovation rencontre un large succès, réside donc dans la capacité des concepteurs à jeter un pont au-dessus du gouffre au fond duquel échouent 80% des innovations (« crossing the chasm »).

<sup>93</sup> Les liens entre les tenants de l'ANT et Philippe Mallein ne participent pas seulement de rapprochements théoriques ou méthodologiques. Il faut aussi lire dans la biographie de Mallein un moment d'appartenance à des réseaux qui ont structuré l'émergence des STS en France, notamment avec l'institutionnalisation du champ de recherche à travers le lancement du programme STS du CNRS en 1980. En effet, il a été chargé de mission à la Direction Générale de la Recherche Scientifique et Technique de 1976 à 1978. La DGRST a financé PAREX, programme franco-britannique dédié aux problèmes de technologie et de développement et aux recherches historiques et sociologiques sur les sciences. Le programme, initié en 1970, est un prélude à la création de l'EAST (European Association for the Studies on Science and Technology). Mallein fait également partie de l'équipe originelle du bulletin « Pandore » avec Michel Callon, Bruno Latour et François Billon, dont le rôle structurant a été fort dans le champ des STS. Pour plus de renseignements sur la structuration du champ en France, on pourra consulter (Kreimer, 1992)

<sup>94</sup> « Rompant avec la tradition, notre grille d'analyse peut avoir quelque utilité en accompagnant le plus en amont possible, dès la conception, le processus de réalisation et de "mise en usage" du nouveau produit/service. (...) Nous avons pu constater que notre grille d'analyse constituait un outil méthodologique efficace pour une bonne collaboration entre ingénieurs et sociologues. » (Mallein & Toussaint, 1994 p. 330-331)

valorisée sous forme commerciale, est ainsi localisée en un endroit où la critique scientifique n'a qu'un faible écho. La performance de la méthode, ainsi que sa viabilité, a moins pour étalon de mesure la somme de critiques qui peuvent provenir des chercheurs travaillant sur l'« usage » que les succès commerciaux attribués à l'utilisation de la méthode. La méthode, outil commercial, est, comme dans le cas de la plupart des outils à la base des prestations de service/conseil, une boîte noire dont seuls les grands mécanismes sont dévoilés comme indices de son fonctionnement. A défaut, son succès commercial serait menacé. Dès lors, on comprend que les mécanismes d'évaluation académique perdent en pertinence voire en opportunité (norme d'universalisme), que les restrictions portant sur les résultats de la méthode – confidentialité des études – posent problème (norme de scepticisme organisé), que le fait que l'opposition entre « cohérence sociotechnique » et « rationalité technosociale » ait pu être transformée en argument de vente soulève des questions (norme de désintéressement), que la création d'une structure commerciale ad hoc, voire l'attribution du cristal à Philippe Mallein exaspère (norme de communalisme). Au fond, ce sont l'ensemble de ces écarts à la norme qui fondent l'exclusion<sup>95</sup> de Philippe Mallein et son équipe du champ scientifique<sup>96</sup>. En somme, CAUTIC<sup>TM</sup> cristalliserait un déséquilibre total entre normes conventionnelles et contre-normes<sup>97</sup> (Mitroff, 1974), au profit tout entier de ces dernières.

Sur le plan instrumental, CAUTIC<sup>TM</sup> détonne également avec la norme alors en vigueur. Examinons tout d'abord l'un des deux outils de la méthode : les profils d'utilisateurs. Contrairement à la planche des critères CAUTIC<sup>TM</sup> qui, pour critiquable qu'elle soit, est une forme de systématisation et de réduction en modalités de certains des enseignements de la « sociologie des usages », la source d'inspiration des profils d'utilisateurs tranche avec les fondements théoriques de ce courant. L'incorporation du paradigme diffusionniste peut entrer en contradiction avec le fait de considérer l'usage comme un construit social (Boullier, 1989). D'abord, parce que le terme de diffusion suppose une étude a posteriori d'une innovation considérée comme stabilisée. Ainsi, bien que CAUTIC<sup>TM</sup> se place en amont du processus de diffusion, la méthode reprend à son compte des enseignements théoriques élaborés à partir d'une innovation considérée comme stabilisée. Néanmoins, ce premier élément critique renvoie plus à la cohésion des sources de

<sup>95</sup> Une exclusion motivée à la fois par les « outsiders » et les « entrepreneurs de morale ».

<sup>96</sup> Nous avons été témoin, lors d'une réunion de travail, de la déclaration suivante, faite par un membre éminent de l'école française des usages : « ça fait vingt ans que Philippe Mallein a cessé de faire de la science, ça me dérange pas, mais bon, qu'il se positionne clairement ! »

<sup>97</sup> Pour rendre compte des comportements scientifiques, Mitroff a souligné le jeu entre des normes conventionnelles et des contre-normes dont l'entêtement au service de ses propres intérêts, le lien fort entre la validité et le producteur de la découverte, l'engagement émotionnel et passionnel, l'investissement moral des conséquences du travail scientifique, la capacité à juger à partir de preuves incomplètes, etc.

la méthode qu'au caractère transgressif de celle-ci. Il est cependant utile de comprendre que la violation de la norme, lue à partir de l'outillage de la méthode, renvoie directement au soubassement théorique partagé par les tenants de l'approche par l'usage. Rappelons-le, l'« école française des usages », dans son travail de réhabilitation de l'usager comme doté de compétences, d'un sens tactique, a exclu toute possibilité de considérer celui-ci à travers le prisme d'une figure docile, empreinte de passivité. Or, en incorporant des éléments diffusionnistes dans son outillage, la méthode CAUTIC<sup>TM</sup> rapatrie cette dernière figure : certains profils sont plus résistants que d'autres au changement et ces résistances sont comprises comme des freins à la diffusion de l'innovation. En somme, la méthode participe également d'un déterminisme technique, bien moins affirmé que ceux que l'on peut retrouver en des lieux où les variables sociologiques n'ont pas voix, mais un déterminisme technique tout de même.

Par ailleurs, la méthodologie employée (entretiens semi-directifs, planche des critères CAUTIC<sup>TM</sup> et grille d'analyse) est mobilisée à des fins de conseil sur un modèle « go/no go » privilégiant l'évaluation de l'acceptabilité de l'innovation à l'étude des usages. Ici encore, la transgression réside dans l'affront fait au credo de l'« école française des usages » : le réductionnisme de la méthode est autant ciblé que l'absence d'explicitation des limites d'un réductionnisme que d'aucuns voient inévitable. Tandis que le projet politique de l'école française des usages visait à rendre compte de la variété des « arts de faire » et d'en sonder les ressorts afin de réhabiliter la créativité et l'indépendance de l'usager, la méthode CAUTIC<sup>TM</sup> renverse la logique. Les ressorts (les profils d'utilisateurs) deviennent un terreau d'accueil figé et les usages, d'objet à observer, deviennent des objets à concevoir. En ce sens, ce n'est pas la granularité et la diversité des usages qui intéresse CAUTIC<sup>TM</sup> mais bien la capacité de l'innovation à répondre à ces caractéristiques de l'usage. La différence est ténue mais elle est au cœur de la compréhension du caractère transgressif de la méthode. Une fois encore, il ne s'agit pas ici de nier le développement d'activités visant à développer une « connaissance stratégique des usages » (Boullier, 1997) chez les grands commanditaires d'études dès les premiers pas de l'« école française des usages » mais plutôt de souligner le fait que si cet affranchissement à la norme pouvait demeurer secrètement déviant et être justifié par l'évolution des structures de financement, la méthode CAUTIC<sup>TM</sup> marque le passage vers une forme de déviance pleinement assumée<sup>98</sup>.

<sup>98</sup> « Au moins Mallein est-il convaincu de “rendre service à la société” et de ne pas “trahir” son métier de chercheur. Beaucoup d'autres font ce passage au conseil moins professionnellement et moins ouvertement. » (Jaureguiberry, 2008 p. 39)

## ***B - L'apprentissage social : Philippe Mallein, point de ralliement d'une science entrepreneuriale***

Pour comprendre la manière dont l'apprentissage social de la déviance s'est effectué, nous avons choisi de revenir sur le parcours de la méthode CAUTIC<sup>TM</sup> à travers l'action de Philippe Mallein<sup>99</sup>. En effet, la question à laquelle nous souhaitons répondre est celle de la manière dont un collectif s'est fondé autour de sa personne et sonder, ce faisant, les caractéristiques de ce collectif.

Pionnier des études d'usages des innovations technologiques au début des années 80 avec le magnétoscope comme objet inaugural, Philippe Mallein, économiste de formation, multiplie les incursions sociologiques dans divers terrains. Y sont abordés, sous l'angle de l'usage et de l'appropriation de l'innovation, les TIC, la domotique et la profession agricole. Sur ces questions, Philippe Mallein devient alors l'interlocuteur privilégié de diverses institutions qu'il s'agisse des pouvoirs publics Rhône alpins (évaluation de l'acceptabilité de mesures novatrices comme le contrat de ville, les états généraux de l'agglomération grenobloise, *Grenoble Campus ouvert*, *Prêt à rentrer étudiants*, etc.) ou d'organisations du monde socio-économique (notamment le Centre Scientifique et Technique du Bâtiment – CSTB ou encore Télé Promotion Rurale). Ingénieur de recherche au CNRS depuis 1978 et membre du CERAT<sup>100</sup>, Philippe Mallein initie en 1996 un programme triennal de recherche hébergé par la Maison des Sciences de l'Homme Alpes (MSH Alpes) et baptisé CAUTIC<sup>TM</sup>. Ce programme réunit des chercheurs d'horizons disciplinaires variés<sup>101</sup> (économistes, psychologues, sociologues, ergonomes, gestionnaires, linguistes, ingénieurs, psychiatres) ainsi que des partenaires d'organisations privées (Schneider Electric, France Télécom, EDF, Le CSTB, le Mouvement Français pour la Qualité,...). Les ateliers organisés débouchent sur la création de la société Ad Valor, chargée de valoriser commercialement la méthode et dont Philippe Mallein est le conseiller scientifique. Cette start-up a bénéficié du soutien de l'incubateur GR-A-IN<sup>102</sup>. Philippe Mallein deviendra même secrétaire du bureau de cet incubateur et sera nommé chargé de valorisation des activités scientifiques à l'Université Pierre Mendès France. Il développera, dans le même temps, un nouveau programme de

<sup>99</sup> La partie consacrée à l'organisation et à la désignation publique s'appuiera également sur la description de ce parcours.

<sup>100</sup> Centre d'Etudes et de Recherche sur l'Administration et le Territoire. Le laboratoire grenoblois est fondé par Jean-Louis Quermonne en 1965 et est désormais intégré à l'UMR PACTE-CNRS.

<sup>101</sup> Une partie de ceux-ci occupent aujourd'hui des postes de chercheurs ou d'ingénieur de recherche au sein d'organisations diverses : CEA-LETI, ERT Umanlab, Ad Valor, Ixiade

<sup>102</sup> Grenoble Alpes Incubation (GR-A-IN), est un incubateur opérationnel créé dans le cadre de la loi sur l'innovation et la recherche, fondé le 29 avril 1999 par le Commissariat à l'énergie atomique (CEA), le Centre national de la recherche scientifique (CNRS), l'Institut national polytechnique de Grenoble (INPG), l'Université Joseph-Fourier (UJF) et l'Université Pierre-Mendès-France (UPMF).

recherche dénommé DICAU (Dispositifs d'Interaction, Cognition et Analyse sociologique de l'Usage) visant à engager CAUTIC™ dans une voie encore plus interdisciplinaire. Ce rapprochement de plus en plus intense avec les organisations industrielles a conduit Philippe Mallein à faire partie des fondateurs du MINATEC IDEAs Laboratory®. Il occupe aujourd'hui le poste de conseiller scientifique auprès du directeur du CEA-LETI.

Le parcours de Philippe Mallein nous montre tout d'abord comment le comportement déviant procède d'un changement dans la répartition des rôles sociaux du scientifique. Tandis que durant l'« école française des usages », le scientifique valorisait un étiquetage qui soulignait sa qualité de chercheur, producteur et développeur d'un champ de connaissances, Philippe Mallein fait usage de cette qualité comme un gage de légitimité et de validité de sa méthode. C'est son expérience et son rôle dans l'« école française des usages » qui lui assurent une crédibilité à endosser les costumes d'administrateur, de régulateur, d'entrepreneur et de conseiller scientifique ; ces dernières responsabilités prenant progressivement le pas sur l'activité de recherche en tant que telle.

Par ailleurs, la mobilisation d'équipes provenant de disciplines diverses durant les programmes CAUTIC™, DICAU puis au MINATEC IDEAs Laboratory®, relève d'une volonté de proposer à la société des solutions abordant plusieurs pans de problèmes considérés comme complexes. Le cloisonnement entre les sciences est compris comme un frein à la mobilisation nécessaire de ressources diverses. En somme, la promotion d'un travail interdisciplinaire puise sa justification dans l'analyse du problème, celui-ci étant défini comme celui de l'acceptabilité de l'innovation et non plus comme l'usage d'une innovation (Brugidou & Jobert, 2008).

Aussi, ce travail interdisciplinaire emprunte un modèle fusionnel. En contraignant les partenaires aux projets à se montrer loyaux (Hirschman, 1974), c'est-à-dire à adhérer à l'éthos de la science sur lesquels ils reposent, ceux-ci acceptent de concentrer leurs efforts sur une finalité commune répondant à une définition du problème, un « cadrage » pour reprendre la terminologie goffmaniène, commune. En somme, CAUTIC™ aplanit l'hétérogénéité disciplinaire des partenaires par les qualités intégratrices de la méthode en tirant profit de l'équivocité du concept d'« usage ». La conception assistée par l'usage, n'est pas une conception assistée par la sociologie, la psychologie ou l'économie.

Enfin, CAUTIC™, en tant que produit de la recherche s'inscrit dans des axes et des marchés de diffusion qui caractérisent un « régime de recherche utilitaire ». En effet, ce régime est constitué par des populations hétérogènes qui appartiennent à différentes institutions telles que *« universités, mais aussi organismes de recherche appliquée,*

*entreprises, ministères techniques, sociétés de conseil, centres techniques industriels, associations professionnelles ou citoyennes.* » (Vinck, 2007 p. 98). Ce régime est également caractérisé par l'orientation de la recherche vers la résolution de problèmes concrets et la posture flottante des personnes qui y évoluent entre « *spécialisation scientifique et le milieu où [elles] s'engage[nt].* » (p. 98) Cette capacité de CAUTIC™ à convaincre de son utilité et de son efficacité tient notamment du travail de stabilisation des figures de l'utilisateur. Celui-ci, réduit à une attitude particulière au changement, catégorisé dans l'un des quatre profils, voit son instabilité identitaire éradiquée :

*« L'utilisateur se retrouve lui aussi souvent dans ce continuum de connaissances mais l'on cherche à tout prix à le stabiliser, à le constituer comme objet quasi expérimental, comme objet de savoir comme objet naturel. »* (Boullier, 1997 p. 1)

L'utilisateur, ainsi stabilisé, offre à chacun des membres du collectif des potentialités de prises sur l'« usage » (Bessy & Chateauraynaud, 1995) moins glissantes que celles disponibles dans chacun de leurs univers propres. Cet avantage concurrentiel de l'approche CAUTIC™ sur d'autres approches plus académiques constitue également « *une remise en cause des modes de connaissance que nous considérons fiables, calqués en fait sur un modèle positiviste de la scientificité.* » (Boullier, 1997 p. 5)

### ***C - La désignation publique : CAUTIC™, une méthode d'intervention engagée***

En terme d'organisation, la méthode CAUTIC™ a émergé à partir de la mise en place d'un programme de recherche qui a reçu le soutien de plusieurs organisations et à plusieurs niveaux. Son avènement participe de l'intensification des relations entre industriels et monde académique au sein de dispositifs qui « combinent des relations de confiance, des liens affectifs, de la crédibilité scientifique et des procédures juridiques » (Vinck, 2007 p. 99) Ces programmes de recherche constituent des dispositifs offrant à l'ensemble des partenaires des moyens d'explorer à la marge de la raison d'être de leurs institutions respectives tout en conservant un pied à l'intérieur de celles-ci.

Le succès de la méthode participe de deux éléments : son adéquation aux demandes formulées par les partenaires économiques et sa conformité aux exigences d'un champ sociologique en pleine mutation. Ces deux éléments sont à la fois constitutifs 1) de l'émergence de la méthode, 2) de son succès.

Abordons tout d'abord la question des sollicitations du monde économique. Didier Vrancken note que la libéralisation des marchés est marquée par le basculement d'une recherche orientée vers le « vrai<sup>103</sup> », le « légitime », vers des dimensions à la fois moins stables et plus ponctuelles :

*« Si l'expertise attenante à l'Etat-providence mobilisait les catégories du vrai, du légitime, elle semble aujourd'hui davantage mobiliser des dimensions plus prospectives et créatives à travers la quête de dispositifs participatifs, de montages de projets, de formes d'accompagnement des politiques publiques toujours à renouveler et à inventer. »* (Vrancken, 2004 p. 38)

On assiste dans le même temps à un mouvement de professionnalisation de la recherche (Papon, 2001) entamé au début du XX<sup>ème</sup> siècle, à la suite de la révolution industrielle, et qui s'intensifie au lendemain de la seconde guerre mondiale. L'une des répercussions de ce mouvement sur l'organisation de la recherche est la généralisation des structures de R&D<sup>104</sup> au sein des organisations industrielles. Cependant, la crise économique a changé la donne en vulgarisant le recours à la sous-traitance de ces activités :

*« La crise économique de la fin du XX<sup>ème</sup> siècle et le dégraissage des structures ont provoqué la suppression de nombreux laboratoires et conduit à faire sous-traiter la recherche par des laboratoires publics. Du coup, la question de la coordination prend de l'importance. Industriels et chercheurs n'agissent pas en fonction des mêmes logiques et temporalités, ils sont conduits à mettre en place des dispositifs dans lesquels ils combinent des relations de confiance, des liens affectifs, de la crédibilité scientifique et des procédures juridiques. Ces ressources instaurent une symétrie entre le laboratoire et l'entreprise pour la répartition du travail, le partage des informations, les échanges de matériaux, la codirection de thèse et la circulation des personnes. »* (Vinck, 2007 p. 101)

C'est parce que la question de la coordination des activités de recherche s'est retrouvée au centre des préoccupations des industriels que des méthodes comme CAUTIC<sup>TM</sup> ont pu trouver un écho favorable parmi un public large et varié. La mobilisation de la méthode s'insère aisément dans des logiques-projet de convocations ponctuelles de

---

<sup>103</sup> « In the late twentieth century academy, "the search for truth" is not concerned with "absolute truth" as conceived by classical philosophers, but rather with an ongoing engagement in a process for *reducing uncertainty* about subjects or phenomena. A central premise of this position is that any conceptual model or finding represents only a partial explanation of reality which can be usurped by new findings at any time. In this environment, theory and experiment are interdependent processes in formulating bodies of knowledge that can be said to *reduce uncertainty*. » (Strickler, 1999 p. 29)

<sup>104</sup> « Ce concept unificateur est apparu au début des années 60, lorsqu'on s'est attaché à mieux caractériser les différentes étapes de la recherche scientifique et technique et à quantifier les ressources humaines et financières qui y étaient engagées. La R&D englobe l'ensemble des activités scientifiques et technologiques qui produisent des connaissances et qui s'appuient sur les savoirs acquis pour mettre au point des techniques nouvelles, engager des processus innovants et développer toutes sortes d'applications » (Papon, 2001 p. 8)

ressources répondant à des problématiques *ad hoc*. Ainsi, les contrats de financement de la recherche passent du statut de moyen à celui de fin en soi : la réponse à la demande formulée est identifiée à l'activité de recherche. En se basant sur le cas du service de R&D de France Télécom, Christine Defuans inscrit le recours à ces méthodes comme participant d'une logique de rationalisation intense de processus de conception dont l'« usage » est une variable dûment banalisée<sup>105</sup> :

*« Les enjeux majeurs en ce qui concerne la dialectique sciences humaines et sociales/ conception de services sont désormais :*

- *De raccourcir les délais qui séparent l'innovation technique de sa transformation en innovation de service*
- *De réussir à développer conjointement les supports, les contenus et les usages*

*La sévère compétition nationale ou internationale sur les services de télécommunications n'autorise en effet ni à être en retard d'un service ni à proposer un service qui ne répondrait pas totalement à la demande de la clientèle. [...] Telles sont les préoccupations qui émergent au début de la décennie quatre-vingt et qui ont permis de fonder des collaborations originales entre spécialistes d'origines diverses et peu habitués à travailler ensemble. »* (Defuans, 2006 p. 88-89)

Cette normalisation fait de la question de l'insertion sociale des techniques non plus une lutte académique mais un objet de conquête industrielle et mercantile<sup>106</sup>. Ici, l'appropriation de l'« usage » par les organisations concernées est facilitée par le développement de méthodes comme CAUTIC™ : standardisées, mobilisant un langage non jargonnant, productrices de résultats opérationnels, ces méthodes constituent un outil de coordination et de collaboration attrayant pour réunir des spécialistes d'origines diverses.

Non sans lien, la question de la diversité nous permet d'aborder le deuxième élément évoqué : la conformité de la méthode aux exigences d'un champ sociologique en pleine mutation. Odile Piriou (Piriou, 2006 ; 2008) considère que la sociologie moderne – de

---

<sup>105</sup> « Depuis les années 2000 la sociologie fait ainsi partie d'une économie dans laquelle la connaissance représente la principale ressource. Ces connaissances – informatique, recherche et développement, marketing, formation et conseil –, que l'on regroupe sous le terme d'investissements immatériels, obéissent à une logique radicalement opposée à celle qui caractérise les investissements classiques. Elles n'interviennent pas directement dans le processus de production mais en amont et en aval de celui-ci. Elles n'obéissent pas à une rationalité fondée sur le coût de leur utilisation – que coûte une intervention sociologique ? Est-elle plus efficiente qu'un investissement informatique ? – mais à une rationalité fondée sur le risque négatif : si je ne réalise pas cette intervention sociologique, je risque de ne pas comprendre un élément central du fonctionnement de mon organisation. [...] De tous ces points de vue, la sociologie ne correspond plus à une perspective d'action et d'investissement extraordinaire. » (Alter, 2008 p. 133-134)

<sup>106</sup> « Si pour l'entreprise, l'innovation ne peut être pensée sans intégrer la dimension marketing ou commerciale du marché, elle ne peut se passer non plus d'une anticipation sur les conséquences micro ou macro sociales de son lancement sur un marché. Encore une fois, afin de limiter les risques d'échec d'un nouveau service, de nouvelles logiques se sont petit à petit imposées dans le champ de la conception de services. Le thème de l'insertion sociale des techniques par exemple, entre dans le champ de ces logiques. » (Defuans, 2006 p. 88)



l'après guerre à nos jours, a vécu trois tournants. Un tournant « scientifique » caractérisé par la généralisation de la sociologie d'enquête et la structuration de la discipline au CNRS ; un second tournant, celui de « l'université de masse » et enfin, depuis les années 2000, un « tournant praticien » caractérisé par « *une croissance rapide d'emplois dans les secteurs non académiques (privés et publics), qui requièrent une expertise et des compétences de sociologie appliquée* » (Piriou, 2008 p. 123) .

La méthode CAUTIC<sup>TM</sup> s'inscrit dans le mouvement d'essor de cette sociologie praticienne qui modifie à la fois l'activité du sociologue et son identité professionnelle. Inspirée par les travaux de Catherine Paradeise sur le processus de professionnalisation de la médecine, Monique Legrand relève trois indicateurs permettant de comprendre l'adaptation des pratiques d'intervention sociologique à l'évolution de la demande sociale : la reconnaissance d'un besoin qui « *s'accompagne d'une prise en charge par les instances de gestion économique (entreprise) et de décisions politiques (Etat) d'une part (1), d'une adaptation des modalités d'intervention sur la base d'une critique des pratiques anciennes d'autre part (2) et enfin, de l'existence d'un nombre suffisant de professionnels (3).* » (Legrand, 2004 p. 83) La méthode CAUTIC<sup>TM</sup> et les personnes ayant concouru à sa diffusion répondent positivement à chacun de ces critères. D'abord, elle est intrinsèquement coordinatrice de l'activité de plusieurs univers sociaux, ce qui n'est pas sans influence sur l'étiquetage déviant que nous nous attachons à démontrer<sup>107</sup>. Aussi, elle s'est autant constituée sur un large réseau d'intervenants que sur l'émergence d'une population de jeunes sociologues prêt à s'affranchir d'un avenir à l'horizon exclusivement académiquement<sup>108</sup>. La méthode CAUTIC<sup>TM</sup> a donc bénéficié d'un recours croissant à formes interventionnistes de la sociologie. Son développement, en s'inscrivant dans une période de recours global à l'« expertise distribuée<sup>109</sup> », offre une forme de coordination alors valorisée qui renouvelle le cadre d'exercice de la sociologie. La recherche est ainsi toute entière dédiée à l'établissement de diagnostics, activité que la méthode peut traiter

<sup>107</sup> « La mise en confrontation d'acteurs dépositaires de représentations et d'enjeux différents dans l'espace de l'intervention revient à activer leurs rapports politiques. Dans cette conception, la sociologie, comme connaissance produite et comme démarche, devient un instrument de « politisation » de la situation sociale étudiée. Par conséquent, le sociologue « s'engage » en engageant sa production sociologique dans ces jeux d'activation des forces sociales. Quel statut donne-t-il alors à son rôle d'acteur ? Comment accorde-t-il le principe d'indétermination du changement social avec les limites de son propre pouvoir sur la situation ? N'invoque-t-il pas avec quelque facilité un détournement de la démarche de changement dans les cas où il perd prise sur les situations qu'il a lui-même contribué à générer ? » (Uhalde, 2008 p. 105)

<sup>108</sup> Nous verrons dans le chapitre suivant comment ceux-ci vont devenir les moteurs d'une nouvelle forme déviante d'utilisation de la notion d'« usage ».

<sup>109</sup> « Nous serions entrés dans une période où « la sociologie participe en fait d'un mouvement plus global de recours à l'expertise et la formulation correcte serait : pas de débats sans plusieurs spécialistes de disciplines différentes. Par une expertise distribuée, on entend (...) une expertise dont chacune des composantes est structurellement incomplète et a donc besoin des autres pour produire le jugement attendu » (Trépos, 2001). » (Legrand, 2004 p. 92)

systematiquement sans s'encombrer des lourdeurs et lenteurs inhérentes à l'activité académique classique :

*« Le diagnostic sert à réaliser un état des lieux (populations, difficultés, structures) et du contexte sur la base duquel les réformes seront engagées. Dès lors, dans le cadre d'une sociologie praticienne, le diagnostic devient outil d'anticipation et d'action pour la mise en œuvre de nouvelles gestions de l'emploi, la réorganisation de structures associatives ou la mise en place d'un nouveau plan urbain. Il est plus ou moins formalisé ou approfondi. Le facteur « temps » est primordial. S'il n'est pas conduit par des chercheurs du monde universitaire ou scientifique, il est adapté à la rationalité des commanditaires, remodelé dans la forme et le contenu, ainsi qu'instrumentalisé par les préconisations pour répondre aux besoins d'opérationnalisation du commanditaire. » (Pirou, 2006 p. 58)*

En sus de considérer le diagnostic comme fin, l'analyse du sociologue est également soumise à une épreuve de « véridiction » (Pirou, 2006). Non seulement son analyse doit apporter des réponses qui « collent » aux objectifs des commanditaires, mais elle doit aussi prouver son caractère opérationnel, être traductible en actions et décisions concrètes. Ce faisant, c'est une fois encore l'autonomie de la science qui s'en trouve ébréchée.

Enfin, cette évolution de l'activité sociologique a des conséquences importantes sur l'identité perçue du sociologue. Celui-ci est alors sensiblement éloigné de l'image de l'intellectuel engagé ou de celle du savant désintéressé. Pour Norbert Alter (2008), cette transformation repose sur deux modifications : celles qui définissent le statut de la sociologie par rapport aux utilisateurs et aux autres disciplines et celles qui transforment la nature même de l'activité. Sans discuter le premier point malgré son intérêt, nous nous concentrerons désormais sur la deuxième modification. Ainsi, Alter considère en des termes durs l'aveuglement du monde académique à l'égard du rapprochement des sociologues au monde économique :

*« Ce phénomène majeur est largement ignoré et par les pouvoirs publics et par les universitaires eux-mêmes, qui continuent souvent à répandre le prêchi-prêcha sollicitant l'intégration de la sociologie dans les pratiques économiques, politiques et sociales. On se trouve devant un paradoxe étonnant, construit d'une part sur la mobilisation de la sociologie – par elle-même et par ses commanditaires – et d'autre part sur l'immobilisation du discours concernant l'utilisation et l'utilité de la sociologie. » (Alter, 2008 p. 134)*

Cet étiquetage qui consolide par omission la qualité déviante des promoteurs de la méthode CAUTIC™ procède notamment du malaise quant à la forme d'engagement prise

par ceux-ci. En effet, au-delà des activités d'analyse qui leurs sont demandés, les sociologues sont enjoins à prescrire et mobiliser. Ces deux activités, auxquels la méthode CAUTIC™ répond favorablement, sont l'expression d'une proximité et d'un engagement clairs auprès des concepteurs qui marquent une rupture épistémologique difficilement supportable pour certains. Paradoxalement, cette forme d'engagement est sollicitée en vertu de l'apport critique de la méthode CAUTIC™ et de la distance qu'elle apporte relativement aux manières *technocentrées* de faire de la conception technologique. Ce paradoxe entre engagement « partisan » et capacité critique reconnue est aplani par la désignation de cette activité comme « instrumentalisée » et en ceci déviante<sup>110</sup>. Au sociologue ayant pour horizon professionnel le « métier de sociologue » (Bourdieu, Chamboredon & Passeron, 1983), au sociologue critique, utilisateur de la méthode CAUTIC™, s'oppose une figure de praticien situé dans une posture de « médiation contributive critique » (Uhalde, 2008) : fondée sur un rejet de l'asymétrie entre savoir savant et savoir pratique et sur le dépassement de la distance relationnelle qui octroient comme mission première au sociologue celle de faire entrer en débat des acteurs dépositaires de représentations et d'enjeux différents dans l'espace d'intervention.

### ***D - La perpétuation de pratiques et savoir-faire : l'émergence locale d'une relève***

Le succès de l'initiative de Philippe Mallein repose également sur un réseau de « jeunes ambassadeurs » de la méthode CAUTIC™. Hautement diplômés (DEA, DESS ou doctorat<sup>111</sup>) et formés aux rudiments de la méthode, ces praticiens<sup>112</sup> sont présents dans l'ensemble des organisations qui ont contribué au développement de la méthode : *l'Université Pierre-Mendès France* de Grenoble, la *MSH Alpes*, la société *Ad Valor*, le

<sup>110</sup> « Par « instrumentalisation », on entend communément le détournement d'un processus ou d'un objet vers d'autres fins que celles initialement conçues. On y entend aussi, de manière plus affective, un détournement illégitime au regard de valeurs ou de conceptions normatives inscrites dans le processus. [...] L'instrumentalisation ne signifie pas uniquement un changement de cap, mais plus fondamentalement un usage dérivé suscitant la réprobation morale. » (Uhalde, 2008 p. 96)

<sup>111</sup> Trois thèses de doctorat nous renseignent sur les relations ambivalentes qu'entretiennent ces praticiens avec le monde académique. Par ordre chronologique, il y a d'abord le travail de Céline Verchère (2004) qui, bien que portant sur l'usage de drogues en milieu festif, a pour arrière-fondement analytique les profils d'identité situés. Jonas Hoffmann (2007) a, de son côté, intégré la méthode dans un modèle explicatif de l'adoption des TIC dans l'industrie. Enfin, Nicolas Veyrat (2008) a mené une réflexion critique sur l'apport de la méthode dans le champ de la prospective industrielle. Ce travail s'inscrit dans la lignée de ceux-ci.

<sup>112</sup> Bien qu'ils possèdent tous une formation initiale en sciences sociales mais pas nécessairement en sociologie, nous nous appuyons sur la définition des praticiens d'Odile Piriou pour les désigner : « Par « praticiens de la sociologie », il faut entendre les diplômés de haut niveau en sociologie [DEA, DESS, doctorat ou diplôme équivalent en formation continue], qui utilisent les connaissances de sociologie, en dehors de l'université et de la recherche publique (CNRS, INSERM, INRA...). Ces praticiens de la sociologie sont donc rémunérés par une organisation privée ou publique (à l'exception de l'université et des centres de recherche de la fonction publique. Ils peuvent exercer en tant qu'indépendants. Ils ont un statut de droit privé. » (Piriou, 2006 p. 14)

cabinet de conseil en innovation *Faber Novel* ou encore le *CNRS*. Prêchant l'évangile de la méthode auprès du monde académique et industriel, ils ont en également été la cheville ouvrière décomplexée dans leur activité praticienne comme nombreux de leurs camarades contemporains :

*« Contrairement aux années 1980, les jeunes sociologues hautement diplômés (doctorat, Master) envisagent d'autres carrières que celles académiques, souvent adossées à ces dernières. Cette évolution doit être reliée aux changements intervenus dans la seconde moitié des années 1980, au sein même du champ scientifique. »* (Pirou, 2008 p. 126)

L'émergence de cette relève, lien opérationnel entre les différents « cycles de crédibilité » de la méthode, a également bénéficié du contexte particulièrement favorable à l'intégration de l'utilisation pythique de l'usage au sein des organisations industrielles. Comme le démontre Christine Defuans, la volonté d'intégration du client dans les politiques et pratiques managériales n'est pas un phénomène nouveau, bien qu'il se manifeste de manière plus ou moins marquée. Néanmoins, malgré les difficultés d'identification de l'apport des sciences sociales à la rationalisation de l'activité de conception et la confusion régnante sur ce que recouvre la notion d'usage dans le sens commun, des méthodes comme CAUTIC™ se sont inscrites comme moyen, pour les managers, de catalyser l'attention des concepteurs sur les contraintes de marché. En ce sens, sa mobilisation participe également de politiques de communication interne dans lesquelles les usages deviennent « *un véhicule de diffusion d'une vision de l'innovation, élargie à la dimension sociale et commerciale de celle-ci, à une problématique globale incluant l'aboutissement sur le marché.* » (Defuans, 2006 p. 182)

Ainsi, la méthode CAUTIC™, cristallise un ensemble de pratiques fondamentalement déviantes quant à la norme instituée par l'« école française des usages ». Son succès est néanmoins tributaire d'un mouvement de rapprochement des sphères académiques et économiques, contribuant ainsi au triomphe de la méthode sur une scène industrielle, aux ramifications tellement nombreuses qu'elle en influence le « marché de la théorie<sup>113</sup>. » Tout compte fait, les promoteurs de la méthode ont construit non un réseau d'« *harmonisation des pratiques de recherche*<sup>114</sup> » (Vinck, 1992) mais d'harmonisation des études d'usage en

---

<sup>113</sup> « Il existe [...] une sorte de pilotage de la recherche par l'aval : certaines théories y sont considérées comme usées, d'autres au contraire comme une source de renouvellement, et cette conception pèse dans les budgets alloués aux centres de recherche ou à leurs représentants indirects, les consultants internes et externes. Il existe donc un début de marché de la théorie. » (Alter, 1999 p. 102)

<sup>114</sup> « Version solide du forum, il permet aux chercheurs d'échanger des idées, mais aussi des données rendues comparables et complémentaires, grâce au travail d'harmonisation et de normalisation de pratiques de chercheurs, de leur langage et de leurs instruments. [...] Dans le réseau, les productions scientifiques locales circulent et sont aisément

unissant autour d'une méthode et en discriminant au-delà de celle-ci : ce qui caractérise les outsiders.

### III - La projection d'usage, objet d'une pratique sibylline

---

Parce qu'elle a également une prétention oraculaire et qu'elle est agie par des jeunes praticiens formés à la manipulation *pythique* de l'usage, la *projection d'usage* s'inscrit dans la continuité de cette pratique sociale. Elle s'inscrit dans ce que Claeys et Stewart (2009) nomme les « recherches spéculatives sur l'innovation<sup>115</sup>. » Néanmoins, ces sociologues ont peu à peu développé des pratiques à nouveau transgressives de l'« usage » en s'emparant de la notion à des fins sibyllines. Ici, la métaphore utilisée auparavant révèle son utilité heuristique et synthétique. Sabina Crippa, anthropologue du fait religieux antique, nous livre une comparaison éclairante sur les différences entre la Pythie et la Sibille :

*« Au modèle institutionnel, permanent de la Pythie s'oppose la divination occasionnelle, indépendante, nomade de la Sibille. La Pythie est la prêtresse d'Apollon, figure historique située dans un lieu précis : le sanctuaire de Delphes. [...] elle œuvre pour la divinité, parle à sa place, évolue sous sa dépendance et son emprise, ses prophéties dépendent entièrement du contrôle des prêtres qui gèrent le calendrier des consultations et le rituel. Aux questions qu'on lui pose, elle répond par oui ou non selon le système binaire de la « mantique fermée », les réponses suivantes étant réélaborées par les prêtres, consignées sur des tablettes puis archivées. [...] Si la Pythie est l'instrument porte-parole du dieu, la Sibille est, en revanche, le sujet de l'énonciation : sa voix, toujours à la première personne, revendique l'originalité de sa prophétie et le caractère indépendant de ses réponses. Douée de « seconde vue », elle prophétise sans instruments ni ornements, selon le modèle de la mantique ouverte : sa prophétie se produit à l'extérieur [...]. Elle ne répond pas aux questions des consultants. Ses prophéties, en effet, ne sont jamais des réponses, mais des visions [...]. Parfois la Sibille parle, très souvent elle chante ses prophéties, d'autres fois elle écrit, elle compose des vers qu'Homère et Virgile auraient imités. La « coprésence » de la voix et de l'écriture est le trait distinctif de la prophétie de la Sibille. »* (Crippa, 1999 p. 96-97)

Ainsi, la Sibille se distingue de la Pythie par son nomadisme, le caractère sibyllin, original, ouvert et indépendant de ses réponses. Tandis que la Pythie ne s'exprimait qu'en vers, la Sibille combine les formes d'expression et sa voix oraculaire « *chant polyphonique, glossolalie, pure émission sonore [...], davantage qu'une difficulté de communication, évoque les formes possibles de communication et d'expérimentation des limites du langage.*

---

<sup>115</sup> « speculative since it's inventive and involves imagining futures different to the present; research, since it involves scientific methods and the exploration of the unknown and the novel; and innovation, since it is directed at informing and stimulating innovation. » (Stewart & Claeys, 2009)

[...] douée d'un pouvoir qui n'est ni celui d'apaiser la nature ni celui de la dominer, la voix nomade et centrifuge de la Sibylle s'exprime à travers toutes formes de réel. » (Crippa, 1999 p. 101)

Le recours à la métaphore de la Sibylle nous permet ainsi de mettre l'accent sur le caractère à la fois déviant et innovant des pratiques observées dans le travail de *projection d'usage*. Ce travail, qui s'effectue en un même lieu, fait pourtant de l'« usage » un lieu aux pratiques multiples, un « espace<sup>116</sup> » de conception technologique. La déviance procède alors de ces utilisations multiples qui perturbent les normes établies en enrôlant l'« usage » à des fins de représentations, de mise à l'épreuve et de valorisation de l'innovation technologique, points que nous abordons dans la première partie. Ces nouvelles pratiques émergent et se consolident par le fait des jeunes praticiens évoqués, qui ont multiplié les contacts hors du sérail local et développé des modes d'interdisciplinarité adaptés au régime de recherche dans lequel s'inscrit leur travail. Enfin, nous signalerons l'ascendance prise par les organisations industrielles comme autorité de coordination et d'orientation d'une activité qui, par ailleurs, s'incarne institutionnellement sous des formes diverses mais toujours contigües ; cette proximité participant d'un mouvement d'« horizontalisation » des « cercles de crédibilité » à l'intérieur desquels circule le travail de projection d'usage.

### ***A - Le passage à l'acte déviant : des conséquences d'avoir pour dessein l'innovation technologique***

La commercialisation des productions scientifiques est symptomatique d'un mouvement plus large de transformation du paysage académique. C'est dans ce cadre que les organisations du monde économiques intègrent en leur sein des activités de recherche avec lesquelles elles entretenaient jusqu'alors des relations de collaborations ponctuelles. Pour Etkowitz (1998), cela participe de l'émergence de nouvelles normes sociales qui

---

<sup>116</sup> « Est un *lieu* l'ordre (quel qu'il soit) selon lequel les éléments sont distribués dans des rapports de coexistence. S'y trouve donc l'impossibilité pour deux choses, d'être à la même place. La loi du « propre » y règne : les éléments considérés sont les uns *à côté* des autres, chacun situé en un endroit « propre » et distinct qu'il définit. Un lieu est donc une configuration instantanée de positions. Il implique une indication de stabilité. Il y a *espace* dès qu'on prend en considération des vecteurs de direction, des quantités de vitesse et la variable de temps. L'espace est un croisement de mobiles. Il est en quelque sorte animé par l'ensemble des mouvements qui s'y déploient. Est *espace* l'effet produit par les opérations qui l'orientent, le circonstancient, le temporalisent et l'amènent à fonctionner en unité polyvalente de programmes conflictuels ou de proximité contractuelles. L'espace serait au lieu ce que devient le mot quand il est parlé, c'est-à-dire quand il est saisi dans l'ambiguïté d'une effectuation, muté en un terme relevant de multiples conventions, posé comme l'acte d'un présent (ou d'un temps), et modifié par les transformations dues à des voisinages successifs. À la différence d'un lieu, il n'a donc ni l'univocité ni la stabilité d'un « propre ». En somme, *l'espace est un lieu pratiqué*. » (De Certeau, 1990 p. 172-173)

inquiètent l'ordre normatif établi. Il relève notamment des phénomènes d'hybridation entre dynamiques économiques et progrès des connaissances, une adaptation permanente des structures universitaires, la généralisation du travail en équipe, l'interdépendance entre université, Etat et industrie ; tous ces phénomènes sont l'expression d'une quête ultime, celle de l'innovation technologique<sup>117</sup>. Avant d'analyser plus empiriquement les caractéristiques de ce régime de recherche, précisons ce que nous entendons par *projection d'usage* et ce que celle-ci tient de déviant. Pascale Trompette et Eric Blanco ont utilisé le terme projection pour évoquer la carrière sociale des innovations technologiques afin de décrire comment l'incertitude qui entoure la trajectoire sociale des innovations est prise en compte lors des phases de conception :

*« Au no man's land de l'incertitude sur l'appropriation future de leurs objets, les concepteurs ont coutume de substituer l'écriture de formes intermédiaires et de scénarios qui dessinent la trajectoire des objets et préfigurent l'articulation entre choix techniques et chaînes sociales [...]. Anticiper les réseaux de production, projeter les conditions économiques de déploiement des innovations, préfigurer les usages et usagers : l'ingénierie de conception intègre une théorie de l'innovation en désignant quelles sont les parties prenantes, comment faire la cartographie des participants, quelles place leur accorder, quel est leur pouvoir sur le destin des innovations. Si la production de ces représentations intermédiaires, leurs mises en discussion et leur réélaboration continue sont au cœur de l'activité de conception, rien n'est encore dit du processus concret par lequel elles participent à la (re)qualification des propriétés de l'artefact technique : comment ces représentations intermédiaires sont-elles élaborées ? De quelle façon performant-elles le travail de conception ? Quelles tensions suscitent-elles au sein des équipes projets ? »* (Trompette, Blanco, 97-98)

Trompette et Blanco, avec qui nous avons partagé le même terreau empirique, soulignent l'absence d'intérêt scientifique pour les modalités de productions des projections d'usage, lacune que ce travail de thèse ambitionne de combler, fût-elle partiellement. Aussi, ces chercheurs, en posant cette question, tracent les gros traits définitionnels de la projection d'usage. Ce faisant, ils pavent la voie à une mise en hypothèses plus précise de notre investigation : on peut incorporer à notre définition provisoire de la projection<sup>118</sup>, enrichie par l'apport de ces résultats, des segments hypothétiques que l'enquête viendra éprouver.

<sup>117</sup> « [...] l'innovation est avant tout la création de nouveaux arrangements au niveau des sphères institutionnelles qui favorisent les conditions pour l'innovation technologique. » (Vinck, 2007 p. 63)

<sup>118</sup> Pour rappel, la définition provisoire retenue est la suivante : travail de représentation d'écologies socio-techniques au sein desquelles l'usage est mis en scène.



On aura compris que l'imprécision de la technologie et l'inexistence des usages attachés à celle-ci sont caractéristiques du travail de *projection d'usage*. Cependant, la projection émerge tout de même par l'édification d' « *un cimetière assumé de démos en tout genre* » où se peuplent des « *représentations intermédiaires de concepts – scénario, démo, maquette [...]* » qui « *sont quelques-unes des modalités de ce nouveau paradigme de la conception.* » (Trompette & Blanco, 2009 p. 105) Ainsi, le travail de *projection d'usage* consiste à la création de « choses<sup>119</sup> » qui représentent des usagers en prise avec des technologies au sein d'une écologie socio-technique fictive. Cette écologie n'existe pas, elle est la résultante d'un travail de configuration socio-technique, « *arrêt sur image qui fige à un moment donné un agencement social autour d'une technique* » (Vedel, 1994). L'« usage » se retrouve ainsi mis en scène, contenu dans les formes d'une représentation, qui dans l'incapacité d'en référer au réel, s'en rapporte au vraisemblable<sup>120</sup>. En effet, ce travail d'encapsulation de l'« usage » est celui d'une mise en ordre d'un monde, ou plus précisément de réduction du désordre, dont on pense qu'il peut advenir au sein. L'« usage » est ainsi une idée à la fois contenue<sup>121</sup> et révélée<sup>122</sup> par les représentations, la production de celles-ci se révélant indispensable au praticien comme instrument de travail et outil de communication. Représentations stabilisées d'une écologie sociotechnique, celles-ci deviennent, dans le monde réel, des « *mobiles immuables* » (Latour, 1987). Elles ont pour propriétés d'être aussi mobiles qu'immuables, présentables, lisibles et combinables avec d'autres objets. A l'exemple de la carte géographique, elles conservent leurs formes (immuables) tandis qu'elles circulent dans le temps et l'espace (mobile). Ces représentations sont des « centres de calcul » permettant de réduire la distance du vraisemblable à la réalité du projet en faisant venir au monde de la conception un « usage » fictif :

« [...] il faut faire venir le monde en certains points qui deviennent alors des centres ou des points de passage obligé. Très bien, mais sous quelle forme faire venir le monde pour que, d'une part, ce qui est loin, distant et périssable, s'y trouve assemblé, et que, d'autre part, le centre ainsi constitué ne soit pas un formidable embouteillage ? Il faut inventer des

<sup>119</sup> La notion de « chose » est utilisée par Geneviève Teil afin de se dégager de la distinction entre personnes et objets, humains et non-humains Geneviève Teil, 'Arbitrer La Présence Des Objets En Société', in 1er Atelier Des Usages Et De La Consommation Sous L'égide De L'afs Rt11 (ed.), (Paris, 2010).

<sup>120</sup> « Bien que la vraisemblance repose sur la conformité des événements et des caractères aux croyances, aux opinions et aux représentations du réel en vigueur, c'est-à-dire le probable, elle tient donc tout autant à l'organisation logique du récit qui unifie les actions et les articule aux caractères des personnages. Cette nécessité créée par la mise en intrigue contribue d'ailleurs à rendre acceptable ce qui pourrait échapper, à première vue, à l'ordre du probable. » (Mercier, 2009). La notion de vraisemblance est caractéristique de la fiction.

<sup>121</sup> « What we set out to create cannot be mapped or captured completely, suggesting that we may view representations in design as containers for ideas. Formal representations, prototypes, scenarios, and more informal sketches have their strong and weak sides with respect to how they contain design ideas. Yet, we have seen no representations where the ideas are self-contained, which emphasizes the need to look at the intersubjective side of design processes. » (Bodker, 1998 p. 115)

<sup>122</sup> « Sans doute y eut-il à Londres des brouillards depuis des siècles, mais personne ne les voyait, de sorte que nous n'en savions rien. Ils n'eurent pas d'existence tant que l'art ne les eut pas inventés. » (Wilde, O., Le déclin du mensonge, 1889)

*dispositifs qui mobilisent les objets du monde, maintiennent leur forme et puissent s'inspecter du regard. Il faut surtout que toutes ces formes puissent se combiner à loisir et se retravailler de telle sorte que celui qui les accumule dispose d'un surcroît de pouvoir. Alors, et alors seulement, certains points deviennent des centres capables de dominer sur une grande échelle. Dans la suite des recherches, je ne parlerai plus des lieux où se cumulent les mobiles immuables que comme des centres de calcul, sans plus m'occuper de savoir à quels domaines ces calculs ressortissent. » (Latour, 2006 p. 33-34)*

Ainsi, ces « immuables mobiles » circulent. Demeure alors à traiter la question de la finalité de cette mise en circulation pour mieux appréhender le caractère déviant du travail de projection d'usage. Les praticiens engagés dans cette activité s'inscrivent dans la lignée des utilisations précédemment analysées de l'« usage » en ce qu'ils accordent une attention toute particulière à l'usager. Les significations qui émergent et se construisent dans son rapport à la technologie constituent leur centre d'intérêt premier. Cependant, celles-ci sont mobilisées autrement que comme matériau strictement analytique (objet de *poiétique*) ou comme indices de l'acceptabilité sociale de l'innovation (objet *pythique*). Cette fois-ci, les significations d'usage sont utilisées comme matériau ressource pour le travail de conception. Afin de mieux comprendre le changement de fonction allouée à ces significations, il nous faut prendre un détour par les méthodes utilisées par ces sociologues. Nous approfondirons la question des ressorts de ce changement de fonction des significations dans la seconde partie de ce chapitre à partir du rôle joué par les collectifs au sein desquels évoluent ces praticiens.

Ainsi, si l'on se contente pour l'instant de considérer que le recueil de ses significations d'usage est l'étape préalable de leur mobilisation dans le processus de conception, nous butons sur l'écueil que doivent nécessairement contourner ces praticiens : comment recueillir les significations d'un « usage » fictif ? Ou, plus largement, par quels moyens peut-on réduire l'incertitude lorsque ce que l'on recherche participe du vraisemblable et non du vrai ?

En posant les choses ainsi, la question qui découle est celle des conditions de mise en œuvre de la véridiction<sup>123</sup> des procédures déployées : il faut ainsi comprendre la projection d'usage comme orientée dans une logique d'épreuves, logique inhérente à toutes formes de projection :

---

<sup>123</sup> « C'est pourquoi, pour caractériser la forme spécifique que prend l'espace logique des sciences sociales la "vérité" d'une assertion empirique, je préfère parler de "véridicité" ; et de "véridiction" pour nommer le contrôle des concepts, du raisonnement et des rapports aux 'référénts' qui y est mis en œuvre. » (Passeron, 1995 p. 14)

*« A set of activities is carried out in a circumscribed environment that is designed to produce an outcome that gives us information as to the operation of the technology. Testing always proceeds by a process of projection. [...] The act of projection – whether from the present to the future, from the present to the past, from the particular to the general, from the small to the large, or from the large to the small (as in miniaturization) – depends crucially upon the establishment of a similarity relationship. It is assumed that the state of affairs pertaining to the test case is similar in crucial respects to the state of affairs pertaining to the actual operation of the technology. [...] It is the assumption of the similarity relationship that enables the projection to be made and that enables engineers warrantably to use the test results as grounds that they have found out something about the actual working on technology. » (Pinch, 1993 p. 28-29)*

Ainsi, la question cruciale est par quelle épreuve la représentation, qui tend vers le vraisemblable, est prise pour vraie (ce que Pinch nomme « relation de similarité ») dans et après le travail de conception ?

On peut déjà considérer que la représentation est amenée à circuler au sein de deux types de réseaux : celui formé par l'équipe de conception (ingénieurs, ergonomes, sociologues, chercheurs, etc.) et celui qui lie des utilisateurs potentiels de la technologie en développement et l'équipe de conception. C'est ce dernier qui nous intéresse particulièrement ici puisque les utilisateurs potentiels, faits de chair et d'os, sont le chaînon manquant de la représentation. Ils sont autant à construire que l'écologie socio-technique représentée. Ils ne sont pas directement observables, ne laissent pas de traces et ne sont pas clairement définis par les commanditaires. Parce que ces utilisateurs sont l'« allié » le plus évanescent qui soit<sup>124</sup>, on attend également des praticiens qu'ils s'instrumentent pour les rendre suffisamment tangibles et stables afin d'en extraire le matériau nécessaire à la « connaissance stratégique des usages » :

*« De même que la connaissance est produite en relation et qu'elle dépend entièrement des dispositifs (cognitifs, techniques, sociaux) mis en place pour la produire, de même la réalité des usagers futurs dépend des dispositifs mis en place pour les faire exister, tant sur le plan des « savoirs » que dans leur réalité de consommateurs. La connaissance stratégique consiste bien à faire exister ces usagers, selon des médiations différentes selon les moments où ils sont saisis (les abonnés « bien connus » ou des futurs consommateurs « virtuels »). La méthode adoptée pour les connaître devient décisive : d'elle, en effet, dépendent les données*

<sup>124</sup> « Si recherche il y a, c'est bien de celle-ci qu'il s'agit, de cette quête d'alliés de toutes sortes, humains ou non humains, depuis le filament à haute résistance jusqu'aux journalistes chargés d'alerter l'opinion publique... Le laboratoire est un des instruments privilégiés de cette quête tous azimuts. » (Akrich, Callon & Latour, 1991 p. 74)

*recueillies, leur exploitation statistique, leur influence sur la stratégie employée. »* (Boullier, 1997 p. 2)

Pour répondre à notre question, et puisqu'au fond ces pratiques méthodologiques forment le cœur de notre investigation empirique, nous nous limiterons pour l'instant à souligner le caractère innovant et nécessairement transgressifs des méthodes déployées<sup>125</sup>.

Ce processus de « *stabilisation* » (Pinch & Bijker, 1989 ; Bijker, 1992 ; Pinch, 2003) s'effectue donc par l'implémentation de méthodes et d'outils dans le cadre d'activité de conception technologique engageant plusieurs partenaires. Ce qui implique que le travail de *projection d'usage* est nécessairement contraint par les objectifs des projets de conception ainsi que par les agendas de chacun des partenaires (Woolgar, 1994). Aussi, plus généralement, l'activité de conception est essentiellement contingente (Bucciarelli, 1994 ; Sharrock & Button, 1997 ; Vinck, 1999) : cette contingence touche tant l'activité elle-même, les formes de collaboration qu'elle induit que ses productions. En somme, l'activité de conception contraint à concevoir la solution la plus satisfaisante à un problème plutôt que d'en rechercher la solution optimale (Simon, 1960). Ainsi, l'exercice d'une science sociale praticienne dans le cadre de conception technologique n'est pas épargné par ces formes de contingences. Les méthodes et outils déployés sont également affectés par cette impossibilité de viser un optimum dans leur utilisation (Shapiro, 1994). La citation qui suit est issue du carnet de note de Laurence Claeys, sociologue à Alcatel Bell Labs. Elle en a publié des extraits dans un article réflexif sur le travail interdisciplinaire dans l'activité de conception (Stewart & Claeys, 2009). Cet extrait illustre l'obligation pour le praticien de dévier d'une pratique orthodoxe et la frustration qui peut en résulter :

« *“What I hate is that everything should go so quickly. How do you do user research if you have 14 days to prepare ? How can you say something about research when you barely have time to analyze them ? How can you master the methodology used if you do not have time to read? Or do a proper literature study before you start your research.”* (20th November 2006) »

Au-delà du fait que les contraintes temporelles ou celles liées aux exigences du travail interdisciplinaire écornent la possibilité d'un usage conventionnel des méthodes, il nous faut également insister sur le fait que celles-ci sont plus incertaines à la fois dans leur

---

<sup>125</sup> « La connaissance stratégique des usagers passe par une remise en cause des modes de connaissance que nous considérons fiables, calqués en fait sur un modèle positiviste de la scientificité. Un opérateur peut certes, nous l'avons vu, appliquer un programme minimum qui consiste à élargir ses catégories pour penser les usagers, leurs identités et leurs activités. Ce programme-là permettrait déjà de refonder les catégories sur lesquelles travaillent les fournisseurs de connaissance attirés sur les usagers-clients. » (Boullier 1997: 5)

déploiement que dans les résultats attendus. Ces méthodes sont instables car elles convoquent les *entités fuyantes* que sont la technologie en développement, ses utilisateurs potentiels ainsi que l'environnement spatio-temporel d'usage<sup>126</sup>.

Enfin, ces méthodes sont nombreuses et constamment renouvelées dans leur utilisation. Qu'il s'agisse des interviews in-situ, questionnaires, études de laboratoire, analyses de tâches, brainstormings, cultural probes, magiciens d'oz, simulations logicielles, prototypages papier, focus group, étude d'utilisabilité, observation participante, co-conception, chacune de ces méthodes peut être mobilisée indépendamment ou articulée à plusieurs autres<sup>127</sup> tandis qu'aucune de celles-ci ne peut être associée comme caractéristique au travail de projection d'usage. Néanmoins, l'objectif est toujours celui de l'articulation entre ces méthodes, l'utilisateur potentiel et le projet de conception. En cela, ces méthodes créent des protocoles expérimentaux mettant en jeu des dynamiques d'asservissement et d'affranchissement de la technologie en développement et des utilisateurs potentiels :

*« Dans l'ordre des dispositifs techniques, les opérations d'asservissement constituent un procédé descriptif permettant de mettre en exergue la manière dont est assemblé, intégré et qualifié un ensemble d'entités disparates, dispersées et indéterminées, afin de doter un « objet technique » de fonctionnalités, de procédures et de règles d'emploi identifiables par un utilisateur ordinaire. Dans l'ordre des sujets, les opérations d'affranchissement constituent un procédé descriptif permettant de mettre en exergue la manière dont sont élargis, dilatés et accrus les états et les compétences du sujet afin que, doté d'une existence sociale, d'un ensemble de rôles au sein de l'organisation et d'une histoire propre, il puisse se voir doter des attributs de l'usager naturel. » (Cardon, 1997 p. 24)*

---

<sup>126</sup> Evoquant le cas du développement du CSCW (Computer Supported Cooperative Work), Dominique Cardon affirme qu'il est « devenu le lieu d'exploration d'une multitude de méthodologies et de dispositifs visant à établir une « conception centrée usager », « assistée par l'usage », un design, ou mieux un « co-design », « participatif » ou « évolutif ». Ces préoccupations témoignent des difficultés suscitées par la prolifération des architectures et des interfaces coopératives au sein de laboratoires, de l'arbitrage incertain entre les tâches qui doivent être prises en charge par l'utilisateur et celles qui peuvent être déléguées à l'objet technique, de la connaissance imparfaite des compétences manipulatoires dont les utilisateurs sont capables de faire preuve. C'est bien pour ces raisons que les sciences sociales ont été invitées à entrer dans le travail de conception afin d'apporter les connaissances nécessaires à la réalisation de ces arbitrages. Les dispositifs mis en place pour les faire participer à la conception des outils coopératifs permettent d'établir une circulation entre la situation naturelle et le laboratoire (a) et d'incorporer l'expérience des usagers dans les différentes phases du processus de conception (b). » (Cardon, 1997 p. 22)

<sup>127</sup> On se trouve alors loin de la figure du scientifique comme entrepreneur individuel telle que décrite par Olivier Rozenberg dans un exercice de confrontation des utilisations du focus group dans le monde académique et dans le monde économique : « Dans les laboratoires de recherche au contraire, un même groupe de chercheurs est impliqué dans l'ensemble des étapes du processus. C'est en cela que nous parlons d'artisanat. Cette absence de division du travail de réalisation des groupes procède en partie d'une division du travail scientifique (recoupant parfois un clivage de genre) entre quantitativiste et qualitatif : il est rare qu'un même chercheur soit spécialiste des deux types de méthode. Le qualitatif s'apparente à un entrepreneur individuel vis-à-vis de son étude : il a obtenu un budget pour la réaliser, il engage sa crédibilité sur les résultats et se doit ainsi de réaliser la plupart des opérations du dispositif ou de les contrôler étroitement (recrutement, transcription). Tel n'est pas le cas en institut de sondage où les chaînes d'interdépendance sont plus longues et la responsabilité plus diluée. » (Backman & Rozenberg, 2009)

On peut ainsi dès à présent affirmer que, méthodologiquement parlant, la *projection d'usage* est donc aussi un travail de *stabilisation de l'incertain* (l'incertain peut être mis en doute tandis que devant l'inconnu s'échappe toute base de discussion), qui se fait dans un cadre de conception marqué par de nombreuses contingences. Ce travail s'effectue par la mise en place de protocoles expérimentaux innovants dont les formes et les résultats sont eux-mêmes contingents de l'activité de conception. Ces protocoles produisent des représentations d'écologies socio-techniques fictives au service de la conception. Ainsi, le travail de *projection d'usage* se démarque des deux autres formes de mobilisation de la notion d'« usage » en ce qu'il s'accommode du conditionnel pour s'effectuer. Le fait de s'emparer du contingent et de le tenir pour une probabilité vraisemblable grève de déviance le travail de *projection d'usage*.

Une autre différence tient du lieu d'où s'exprime les praticiens. Tandis que nous avons décrit l'émergence d'un véritable credo scientifique concernant l'usage *poiétique* de l'« usage » dans sa première carrière, ces sociologues praticiens sont dans l'obligation pratique d'adhérer à un autre dogme : celui de l'innovation technologique comme facteur de croissance économique. En effet, ces sociologues présentent tous des liens de subordination plus ou moins directs avec le même centre industriel, le CEA-LETI<sup>128</sup>. Le centre de recherche appliquée, « acteur clé au service de l'innovation », se présente comme un véritable moteur de compétitivité :

*« Au cœur du Campus d'innovation MINATEC, le CEA-LETI est un centre de recherche appliquée en microélectronique et en technologies de l'information et de la santé. Interface privilégiée du monde industriel et de la recherche académique, il assure chaque année le développement et le transfert de technologies innovantes dans des secteurs variés. Avec plus de 250 étudiants impliqués dans les activités de recherche, le CEA-LETI est source de compétences dédiées à l'innovation. Fort d'un portefeuille de 1 500 familles de brevets, il contribue à renforcer la compétitivité de ses partenaires industriels. »* (Source : <http://www.CEA-Leti.fr/fr/Decouvrez-le-CEA-Leti/Qui-sommes-nous>)

Ce positionnement implique, en creux, une connotation positive à la technologie, du moins du point de vue des bénéfices économiques attendus du passage de l'invention à l'innovation. Dès lors, l'injonction d'innover se comprend prioritairement comme injonction à produire de l'innovation technologique à partir des inventions qui peuplent les étagères des

<sup>128</sup> Nous reviendrons plus en détails sur les conséquences organisationnelles de cette forte présence d'un partenaire industriel (le CEA est un EPIC) dans la partie C.

ingénieurs et chercheurs en sciences dures. En ce sens, l'« usage » est ici clairement positionné comme une ressource au service de l'innovation technologique.

Notre troisième point est l'instant d'intervention de ces praticiens dans le processus de conception. Tandis que le rayon d'intervention des « sociologues des usages » était posté soit très en amont ou alors en aval du processus d'innovation, le positionnement occupé ici diffère en ce qu'il oblige les sociologues à *plonger les mains dans le cambouis* du processus de conception. On peut expliquer<sup>129</sup> ce tournant vers l'activité de conception par l'essence même des technologies développées par le CEA-LETI (la microélectronique et les technologies de l'information) comme l'affirme Dominique Cardon :

*« Peu d'innovations technologiques sont parvenues à associer aussi étroitement à leur développement les plus « sociales » des sciences sociales, que l'informatique et la télécommunication. [...] A la différence des plus « humaines » des sciences sociales, la psychologie ou l'ergonomie, la sociologie est rarement invitée es qualité dans le laboratoire des innovateurs pour être directement impliquée dans la fabrication de prototypes techniques. »* (Cardon, 1997 p. 15)

Ce travail, qui s'effectue la plupart du temps à partir d'une réflexion sur le devenir de *briques technologiques*<sup>130</sup>, s'inscrit dans un processus double (Koch & Stemerding, 1994 p. 1212) : d'une part, a lieu une activité de spécifications techniques durant laquelle le contenu et la fonction d'une option technique particulière est spécifiée en pratique ; d'autre part, prend place un processus d'articulation de la demande durant lequel concepteurs et consommateurs (représentés ou projetés<sup>131</sup>) spécifient leurs rapports aux options techniques disponibles. Ainsi, l'indétermination est grande concernant la technologie elle-même, son insertion dans un produit final et le public réceptacle de ceux-ci. C'est ce que Trompette et Blanco interprètent comme un « remake » du « drame de l'innovation » :

---

<sup>129</sup> Il nous faut ici souligner le rôle important de la diffusion et de la vulgarisation, au niveau local, des principes de la sociologie de l'innovation et partiellement de l'ANT, dues au travail de sape effectué par le CRISTO (Centre de Recherche sur l'Innovation Socio-Technique et les Organisations industrielles). L'UMR, aujourd'hui intégrée à l'UMR PACTE/CNRS, a été fortement impliquée dans la création de l'École nationale supérieure de génie industriel (ENSGI) et de l'Institut de la production et des organisations industrielles (IPI), respectivement en 1990 et 1999 (voir (Segrestin, 2010). Ainsi, nous reconnaissons que le chemin analytique emprunté néglige autant l'intrication des influences génératrices des rapprochements entre sciences sociales et sciences pour l'ingénieur à Grenoble que les apports théoriques sourds ou revendiqués de la sociologie de l'innovation à certaines pratiques de la sociologie.

<sup>130</sup> L'usage de ce terme est courant au sein d'organisations tournées vers le développement technologique. Il renvoie à des innovations technologiques dont le stade précoce de développement ne permet pas encore de déterminer d'applications précises. Elles sont destinées à être insérées dans un ensemble plus large, le produit final.

<sup>131</sup> « Dans les environnements R&D que nous côtoyons, [la connaissance anticipative de l'usage] s'appuie de façon privilégiée sur la convocation de futurs usagers en différents lieux du processus d'innovation : comme ressource cognitive dans l'élaboration prospective d'usages autour d'une nouvelle technologie, comme co-concepteurs dans la définition des fonctionnalités et la création de la valeur, ou encore comme « figure-test » dans la mise à l'épreuve du potentiel d'appropriation des nouveaux produits. » (Trompette & Blanco, 2009 p. 105)

*« Le drame de l'innovateur se rejoue, mais cette fois à travers une mise en scène distinguant voire opposant : d'un côté les technologues, entrepreneurs de nouveaux horizons technologiques dont ils cherchent à asseoir la légitimité par l'adéquation au marché ; de l'autre, les sociologues en quête de signaux faibles de valeurs d'usage et porteurs d'un processus itératif de (re)qualification des choix techniques au fil des connaissances acquises. » (Trompette & Blanco, 2009 p. 113)*

Ce « drame » achève d'emmener les sociologues plus loin qu'auparavant dans l'exploration d'un territoire indéterminé. Il ne s'agit plus seulement d'observer l'« usage » et de rendre compte de ses dynamiques de construction sociale, ni de prophétiser sur la réussite de l'insertion sociale d'une technologie. Ces sociologues praticiens interviennent comme acteur d'un processus technologique que l'« école française des usages » et la nouvelle sociologie des sciences et des techniques a mis en évidence, la co-construction du social et du technique ; ce cadre technologique (« technological frame ») dont Wiebe Bijker (1992 p. 98) affirme qu'il constitue une charnière entre les perspectives traitant de l'impact social des technologies et celles abordant la question de leur capacité à en être façonnées.

Ainsi, le caractère déviant du travail de projection d'usage se manifeste par un détournement d'usage des normes scientifiques. Celles-ci voient leur statut profondément modifiées ici : elles ne constituent plus le cadre référent à l'intérieur duquel s'effectue la pratique mais le point d'appui de formes de déviations. La supériorité des normes sur d'autres principes d'action peut se trouver anéantie par l'ajustement de la pratique aux contraintes de la conception. S'en trouve profondément modifiée la permanence du statut supérieur de ces normes sur d'autres. En d'autres termes, les normes, selon les contextes, peuvent être ignorées, laissées de côté, utilisées comme source d'inspiration, comme un moyen de contrôle parmi d'autres, comme outil d'analyse réflexive, comme contre-exemple, comme base d'exploration, etc. Le caractère déviant du travail de *projection d'usage* se manifeste ainsi par le fait qu'il émousse le statut permanent et rigide des normes en s'inscrivant dans la contingence, l'incertitude et en s'associant étroitement, jusqu'à s'y hybrider, aux processus de de conception technologique. Ces statuts pluriels et contingents renouvellent la question de leur transmission par le biais des institutions sociales traditionnelles.



## ***B - L'apprentissage social : la prise du tournant expérientiel***

L'apprentissage social de la *projection d'usage* comme mode d'utilisation déviante de la notion d'« usage » est d'abord l'œuvre de jeunes sociologues issus du même sérail. Ils sont quasiment tous rompus à l'exercice de la méthode CAUTIC™. Cependant, s'ils en ont gardé l'objectif d'apporter une forme concrète de réponse à leurs commanditaires, ils ont, dans leur pratiques quotidiennes, développé petit à petit une nouvelle manière d'envisager leur contribution à l'activité de conception.

Ces jeunes sociologues vont emprunter le tournant « expérientiel » pris par certains théoriciens de l'activité de conception (Battarbee, 2003 ; Redström, 2006). Inspiré d'un article au grand retentissement de la Harvard Business Review, dans lequel les auteurs annonçaient l'avènement d'une « économie de l'expérience » en succession aux économies agraire, industrielle et servicielle<sup>132</sup>, le concept a une définition floue dans le cadre de la conception technologique. Cependant, l'accent est mis sur l'importance de la prise en compte des contextes d'utilisation du dispositif technologique, du caractère subjectif et social de la manière de percevoir ce contexte et enfin de la contingence de ceux-ci (Forlizzi & Ford, 2000 ; Battarbee, 2003 ; Vaajakallio & Mattelmäki, 2007). Si le tournant expérientiel marque le dépassement des études ergonomiques et des études d'utilisabilité dans les sciences de la conception<sup>133</sup> (voir partie II), il fait écho aux ambitions portées par la méthode CAUTIC™. Cependant, la différence réside dans la manière de se saisir de l'« expérience ». D'une variable considérée comme condition du succès de l'innovation, l'« expérience » devient, dans le travail de *projection d'usage*, un élément à construire, un objectif de conception :

*« It is now becoming clear, in view of the large number of award-winning designs that have failed the test of use, that the design community's criteria for successful design differs radically from that of design users. Design itself needs to be redefined in terms of peoples' experiences, instead of in terms of objects. This static geometrical criteria of the design of the industrial era must be abandoned in favor of a focus on the dynamic, multisensory experiences of design users. » (Mitchell, 1993 p. 131)*

---

<sup>132</sup> « An experience occurs when a company intentionally uses services as the stage, and goods as props, to engage individual customers in a way that creates a memorable event. Commodities are fungible, goods tangible, and experiences memorable » (Pine & Gilmore, 1998)

<sup>133</sup> « If design used to be a matter of physical form, its subject matter being the material object, it now increasingly seems to be about the user and her experiences. Starting with the social ambitions of modernism and the interest in shaping the use of things, the discourse has developed and expanded. » (Redström, 2006 p. 127)

Ce changement de perspective, s'il peut paraître anecdotique, a plusieurs implications profondes sur le travail du praticien, le statut du savoir produit et les instruments de production de ce savoir. D'abord, il annihile toute velléité de mise en conformité du dispositif technologique en conception aux usagers potentiels, qu'il s'agisse de leurs significations d'usage, de leurs désirs ou encore de leurs compétences. Parce que d'une part, le travail de *projection d'usage* déplace le centre d'intérêt de l'artefact en conception vers la conception d'une « expérience » liée à cet artefact. Comme le contexte est un construit social, il est susceptible d'héberger  $n$  interactions entre  $n$  (pratiques d') humains et  $n$  (perceptions) de  $n$  technologies dans  $n$  situations. En somme, il n'est plus possible de penser un trajet linéaire et diffusionniste qui pose la technologie en point de départ et l'utilisateur en point d'arrivée. Ce qui à l'œuvre, c'est la construction de *projections d'usage* qui mettent en scène un ou plusieurs contextes sociotechniques extraits d'une population infinie de contextes et provoquant un large éventail d'interprétations.

Le travail de *projection d'usage* opère un autre déplacement important du point vers lequel convergent les efforts des praticiens : il décentre l'intérêt de l'objet en conception vers le processus de conception lui-même<sup>134</sup> (Gaver & Martin, 2000 ; Redström, 2006), ce qui fait écho à l'idée de modernité réflexive évoquée en introduction. Le processus de conception est, en somme, volontairement déstabilisé par cette mise en réflexivité nourrie par les ressources externes que sont les expressions des utilisateurs potentiels. L'écart entre usages prescrits et usages observés est intégré comme une donnée non problématique mais *normale*, qu'il ne s'agit ni de dénier, ni de réduire. Dès lors, il n'est plus possible de raisonner en termes de succès ou d'erreurs, de « logiques sociotechnique ou technosociale » mais bien de penser le statut du savoir récolté pour pouvoir le rendre actionnable dans la conception :

*« This is not a question of the ways in which we need to expand existing definitions of usability and methodological frameworks in order to deal with the user experience, this is a question of what knowledge in general can be obtained during the design process. And it is not a question of simply obtaining more knowledge - there are fundamental problems associated with the idea that design is about determining the use of objects in detail. »* (Redström, 2006 p. 135)

---

<sup>134</sup> Ici encore, l'on pourrait embrayer sur les apports de la sociologie de l'innovation, nourrie par la sociologie des usages.  
Emmanuel Anjembe – « La composition de fictions axiomatiques au service de la recherche technologique » - Thèse Grenoble Universités 2014

Ainsi, l'activité de conception est alors envisagée non comme tournée vers la production de solutions mais vers la formulation de problèmes<sup>135</sup>. Le travail de projection d'usage s'envisage alors comme poussant la transformation du lieu de conception en lieu de débats et de disputes (Seago & Dunne, 1999) au sein duquel les utilisateurs potentiels ne sont pas une chambre de validation mais une assemblée de concepteurs, partie au débat. Cette tendance qui, avouons-le tient plus de l'impensé que de la revendication affirmée, pose encore le problème des conséquences de son expression formelle comme le résume Redström à travers ces deux questions :

« What would happen if we used our knowledge about current practices not to answer certain questions by our design, but to avoid answering them? Or, in other words, if we tried to make our design ask questions about use that were open for its users to answer, rather than thinking of the design as a way of providing well-defined answers from the start.” (Redström, 2006 p. 136-137)

Indirectement, ces questionnements appellent l'interrogation de l'articulation des méthodes déployées dans l'activité de projection. S'il ne s'agit plus de dire le bon ou le mauvais, de valider ou d'invalidier, mais de poser des questions, comment qualifier la finalité de ces méthodes ? En vérité, cette question n'est pas vraiment neuve. C'est la question de la résolution de la tension entre « exploration » et « exploitation » (March, 1991), le premier terme consistant en l'affinement et l'extension de compétences existantes et dont les retours sont positifs, prédictibles et immédiats, le second terme privilégiant l'expérimentation et la diversité d'alternatives et dont les retours sont incertains, distants et souvent négativement connotés. Si l'on peut classer le travail de conception selon cette opposition, le travail de projection d'usage mérite cependant une autre distribution. Selon qu'il s'inscrive dans l'exploration ou l'exploitation en termes de dominante de conception, le travail de projection d'usage sera plus ou moins tourné vers l'évaluation du dispositif technologique ou vers la création – c'est-à-dire la conception du dispositif technologique (voir tableau 1). Il devient activité de « pure » création lorsque le processus de conception

---

<sup>135</sup> On peut, à cet égard, citer cet extrait de Jones, véritable plaidoyer pour l'abandon de cet objectif de réduction de l'incertitude en conception :

« But there is a hidden cost, a severe one, which has only recently become evident. It is that of inflexibility, over-specialization, the realization that this 'plastic world' of homogenized, cost-reduced products is increasingly unalterable, un-repairable, and imposes upon us (from its stabilization of the larger scale of functions) a life, an obligatory way of using what is made, that is felt as coercive, not satisfying, with decreasing outlets for individuality. The lesson is obvious, though how to apply it is not: do not stabilize functions. » (Jones, 1988 p. 121)

est exploratoire<sup>136</sup>. Ici, créer signifie alors dépasser le constat d'observation et les préconisations qui en découlent et assumer le rôle de force de proposition avec comme outillage possible, l'observation (Button, Graham & Dourish, 1996 ; Dourish, 2001) ; mais les propositions avancées sont moins des solutions que des cadrages problématiques<sup>137</sup> qui « transcendent » les paradigmes de style, d'usage, technologiques ou économiques (Ehn, 1988)

Tableau 2. La projection entre évaluation et création

		Pratique sociologique	
		Exploitation	Exploration
Conception technologique	Exploitation	Evaluation	Evaluation/Création
	Exploration	Evaluation/Création	Création

Bien que la différence ne soit pas toujours aussi tranchée que l'analyse le présente (Sengers & Gaver, 2006 ; Kaye, Boehner, Laaksolahti & Stahl, 2007), elle nous permet de souligner clairement l'engagement des praticiens comme concepteurs du dispositif technologique dans le cas de la *projection d'usage*. Une forme de « recherche proactive » qu'Yvonne Rogers (1997) appelle de ses vœux :

*« The value of "packaged prescriptive" advice provided by social scientists -- be they cognitive psychologists, ethnomethodologists, or otherwise -- for the purpose of improving system design through applying their theories and methodologies has been questioned. It is argued that approaches putting the onus on designers to translate their advice will remain largely unused and, hence, have little impact. It is time for a change. Rather than always take a backseat role, researchers need to become more proactive in their involvement with the people and objects of their study. This means engaging more in an ongoing dialogue with the various groups of people working or designing together (i.e., the users, the*

<sup>136</sup> On retrouve une typologie similaire mais ternaire chez Fallman (Fallman, 2008). L'auteur distingue ainsi une activité de conception tournée vers la pratique (« Design Practice ») dans laquelle le chercheur est impliqué dans une pratique de conception particulière mais le fait avec une question de recherche préexistante en tête ; l'activité de conception tournée vers l'exploration (Design Exploration) qui se distingue de la première par le fait que la question principale est « what if ? » et l'agenda du chercheur prend le dessus sur l'activité de conception (« design becomes a statement of what is possible, what would be desirable or ideal, or just to show alternatives and examples » p.7) ; et enfin l'activité de conception tournée vers la recherche (« Design studies »)

<sup>137</sup> On se réfère ici à la notion de « problem-setting » chez (Schön, 1992)

*managers, and the designers). Researchers should stop shying away from being involved. »* (Rogers, 1997 p. 69)

Ainsi, la *projection d'usage*, n'a pas, en tant qu'« épreuve » (Pinch, 1993), pour ambition première de renforcer le contrôle de l'adéquation de l'innovation à son terreau d'accueil mais plutôt de rendre tangible, et donc discutable, l'intention de conception<sup>138139</sup>. C'est dans ce contexte que l'interdisciplinarité qui se joue à travers les pratiques de concepteurs aux origines disciplinaires variées est justifiée par la nécessité d'*obtenir du concret* de la conception et se fait « autour d'un instrument, d'un objet ou d'un terrain, la mobilisation de ressources de plusieurs disciplines s'impose parfois. » (Vinck, 2007 p. 84) Cette interdisciplinarité emprunte, dans ses finalités revendiquées, le « modèle de la complémentarité » (Vinck, 2000) en articulant des « compétences complémentaires pour traiter de manière conjointe une question » et en allant « au-delà d'une simple juxtaposition des apports disciplinaires » car « il y a exploration des points d'articulation entre les savoirs en vue d'une réalisation conjointe », le dispositif technologique.

Le tournant « expérientiel » que nous venons de décrire est, au moment de l'écriture de la thèse, encore en voie de réalisation chez les jeunes praticiens. S'il s'affirme de plus en plus dans leurs pratiques quotidiennes, la finalité évaluative des études menées demeure en survivance jusqu'à parfois s'avérer dominante selon les personnes et les organisations concernées. Et, à cet égard, on peut supposer que l'affirmation graduelle de ces pratiques s'est faite par le contact avec des chercheurs et ingénieurs étrangers (notamment scandinaves) chez qui la pratique de la projection d'usage et/ou ses implications épistémiques étaient plus rodées sinon moins stigmatisées comme déviantes du fait de la tradition non-problématique de coopération entre industrie et université dans ces pays-là. En effet, les jeunes sociologues dont nous parlons ont tous participé à plusieurs projets européens d'envergure qui ont enclenché ce processus de remise en question des savoirs et savoir-faire acquis durant le temps de développement de CAUTIC™. Il s'agit, pour les plus importants du :

---

<sup>138</sup> « By making the desired interpretation of the objects obvious and impossible to resist, we aim to design not only the object itself but also the perception, and even the experience, of it. Indeed, the terms 'user testing' and 'user evaluations' can be read in two rather different ways. If we think of this process of becoming users as being a process of inviting and accepting the things that will become the building blocks of our lifeworlds, it is also less clear that this is a process that designers want to or should try to control, compared to when we understand use as a matter of communication of designer intent. » (Redström, 2006 p. 129-130)

<sup>139</sup> Cf. le concept d'objet intermédiaire (Jeantet, 1998 ; Vinck, 1999 ; Boujut & Blanco, 2003) dans la partie 2 de la thèse.

- projet ADAMOS<sup>140</sup> (Adaptive Mobile Services - Design Parameters & User Experience Factors) : projet d'une durée de trois ans (2003-2005) bénéficiant du soutien du RNRT. Le consortium était composé de l'université d'Oulu (Finlande), de l'Université Joseph Fourier (Grenoble), de STMicroelectronics, du CEA-LETI, de VTT, de Hewlett Packard et de France Telecom R&D.
- projet E-SENSE<sup>141</sup> (capturing of Ambient Intelligence for Beyond 3G Mobile Communication Systems through Wireless Sensor Networks) : bénéficiant du soutien du sixième programme-cadre de l'Union Européenne, le projet réunit un consortium de 23 partenaires dont sept partenaires industriels (Telefonica, IBM, Fujitsu UK, Mitsubishi France, Thales UK et EADS), une compagnie de gestion (ALMA), deux pme (HFC, Ambient Systems), quatre instituts de recherche (CEA-LETI, IMEC, CSEM, FhG Fokus) et dix institutions académiques dont l'UPMF.
- Le projet SENSEI<sup>142</sup> (Integrating the Physical with the Digital World of the Network of the Future) : bénéficiant du soutien du septième programme-cadre de l'Union Européenne, le projet a débuté en janvier 2008 pour une durée de trois ans. Il associe 19 partenaires : le CEA-LETI, ARUP, Eriksson, NEC, SAP, Telefonica, Thalès, Ambient Systems, et des institutions universitaires comme l'Université de Surrey et l'UPMF.

C'est au contact de ces chercheurs que les sociologues ont fait basculer leur sociologie praticienne vers la *projection d'usage* et, par là même, inscrite celle-ci dans une logique de diffusion caractéristique du « régime transversal de production des savoirs » (Pestre, 1997 ; Shinn, 2000) dont Dominique Vinck nous offre une synthèse des caractéristiques qui fait particulièrement écho avec l'analyse que nous venons de mener :

*« Les chercheurs s'intéressent surtout à la métrologie et à la méthodologie, ainsi qu'à la conception et la réalisation d'instruments génériques ou de protocoles. Ils se mettent au service de la recherche académique comme du régime utilitaire. Ils ne se rattachent à aucune discipline, mais forment des communautés interstitielles. [...] La diffusion de leurs travaux (instruments et littérature) concerne un large éventail de milieux universitaires, industriels, techniques et administratifs, avec parfois un impact universel. Les membres de ce régime travaillent entre les disciplines et entre les institutions, même s'ils sont nécessairement rattachés à une institution particulière. Leur identité se construit au niveau*

<sup>140</sup> Pour plus d'informations voir <http://www.tol.oulu.fi/projects/adamos/>

<sup>141</sup> Pour plus d'informations voir <http://www.ist-e-sense.org/>

<sup>142</sup> Pour plus d'informations voir <http://www.sensei-project.eu/>

*de réseaux transversaux et hétérogènes. Ils s'insèrent dans des niches et circulent entre divers groupes ; ils évitent de trop se lier à un organisme. Ils permettent de relier des champs scientifiques, technologiques et institutionnels parfois isolés les uns des autres. Ils contribuent parfois à normaliser certaines pratiques au-delà de la diversité des institutions. Dans ce régime, la communauté interstitielle connaît des phases d'ouverture et des phases de discrétion liées à la conceptualisation d'instruments loin du regard et de l'influence des autres groupes. Ce régime est transversal pour au moins trois raisons : les axes de recherche ont des origines multiples ; les espaces de diffusion sont divers ; la communauté se construit en relation étroite avec les trois autres régimes.» (Vinck, 2007 p. 85-87)*

### ***C - La désignation publique : le poids des organisations industrielles dans la structuration de la pratique***

On peut constater, avec Didier Vrancken (2004 p. 26), que l'entreprise a joué un rôle de visibilisation des sociologues qui s'y sont d'ailleurs professionnalisés. Dans notre cas, ce rôle est joué par le CEA-LETI. En effet, l'accélération du rythme de sortie d'innovations, le raccourcissement des cycles de vie des produits, la mondialisation des marchés de diffusion technologies, la hausse des dépenses de R&D nécessaires à l'avènement d'un produit ou d'un processus, le risque de dépenses mal orientées, le mouvement de fusion de technologies sont autant de dynamiques environnementales qui constituent pour des organisations comme le CEA-LETI autant de menaces que d'opportunités et qui augmentent le besoin d'anticipation ; qu'il s'agisse d'identification des tendances technologiques ou de l'anticipation des usages (Reger, 2001). Au niveau national, il convient également de comprendre l'implication de l'inscription de l'activité du CEA sur une scène compétitive mondialisée (Vinck, 2007). Comme de nombreux organismes de recherche gouvernementale créée durant l'après-guerre, la mission du CEA consistait à remplir un objectif d'intérêt général, mission qui n'aurait pu être menée par l'industrie, en raison du manque d'intérêt et d'opportunités commerciales immédiates, ou par l'université, en raison du caractère par trop appliqué de la recherche. Ainsi, l'INRA était chargé du développement agricole, l'IRD du développement, l'INSERM de la recherche sur la santé publique, l'INRETS de la sécurité dans les transports et le CEA était investi de la recherche sur l'autonomie énergétique de la nation. Cependant, la pression des logiques commerciale et concurrentielle a conduit à des profonds bouleversements dans le fonctionnement et les missions de ces organismes. Ceux-ci évoluent désormais dans des univers où entreprises, laboratoires universitaires ou

organismes hybrides sont en compétition sur des problématiques de recherche identiques, et par voie d'extension, sur les financements et la valorisation économique de l'activité. Ainsi, de l'objectif de remplir une ou plusieurs missions d'intérêt général, la vocation de ces organisations est devenue quasi-commerciale et leur « *survie dépend de leur capacité à proposer des services à des « clients » (services publics, entreprises privées, associations de citoyens comme les associations de malades, fondations) ou directement au grand public via la médiatisation des collectes de fonds.* » (Vinck, 2007 p. 94). Dans ce cadre, la mission du CEA-LETI est alors « *moins de produire de la connaissance académique que de mettre au point des concepts opérationnels et les savoir-faire associés destinés à des utilisateurs intermédiaires, industriels notamment, mettant au point de nouveaux produits ou services.* » (Vinck, 2007 p. 94)

C'est donc à la lumière de ces bouleversements et face à cette montée en pression à laquelle doit faire face le CEA-LETI qu'il faut comprendre son investissement dans la promotion d'une sociologie praticienne dans son environnement, comme l'un des moyens de réduction des incertitudes qui pèsent sur la diffusion des technologies qu'il développe (voir introduction). Concrètement, on peut lire dans la prolifération d'organisations dédiées à proximité du CEA-LETI<sup>143</sup> une déclinaison de la puissance de structuration de l'organisation industrielle sur la vie scientifique grenobloise, un pouvoir d'influence qui transcende donc la frontière entre sciences dures et sciences humaines et sociales. Cependant, la prolifération de ces structures peut aussi être interprétée comme l'expression d'une posture hésitante concernant les rapports à développer avec les sciences sociales. En effet, plus qu'une politique clairement affirmée d'intégration des sciences sociales à l'activité de conception – position qui n'est institutionnellement tenue que par le LID et de façon plus ambivalente par le MINATEC IDEAs Laboratory®, le CEA-LETI a mis en place un archipel de structures aux interactions denses : géographiquement proches, elles engagent des partenariats avec des acteurs identiques et/ou poursuivant des objectifs plus ou moins similaires, ce qui favorisent l'intensité des échanges entre praticiens respectivement rattachés à des entités différentes, ce qui fera l'objet de la dernière partie de ce chapitre.

Cet adossement de la sociologie praticienne au CEA-LETI est autrement intéressant si on le considère au regard des effets induits sur l'étiquetage des pratiques déviantes. En nous basant une nouvelle fois sur notre expérience personnelle de doctorant hébergé par le LID, nous avons relevé que l'archipel d'acteurs de la sociologie praticienne qui gravitent dans l'environnement du CEA-LETI est rarement désigné par les chercheurs en sciences sociales

<sup>143</sup> Voir Introduction



du campus par sa diversité mais plutôt envisagé comme un bloc monolithique prenant place sur le campus ouest de Grenoble<sup>144</sup>. Les praticiens y sont désignés variablement mais toujours sous la bannière commune du CEA comme « les sociologues du CEA », les « gens du CEA », les « consultants du CEA », les « chercheurs/ingénieurs du CEA », etc.... Autrement dit, leur proximité géographique et institutionnelle avec le CEA suffit à la caractérisation de leurs pratiques comme déviantes, car affranchies du patronage académique traditionnel.

Enfin, il faut relever que cette confusion qui réduit la diversité des lieux de pratique règne également à l'intérieur même de la communauté des sociologues praticiens. En effet, nous avons assisté plusieurs fois à des discussions au contenu cocasse portant sur la manière de se présenter en tant que praticien. Si la fonction attachée au poste de l'institution de rattachement permet parfois de couper court au débat (ingénieur-chercheur, ingénieur de recherche, chargé d'étude), la question du positionnement disciplinaire le ravive. Ainsi, lorsque certains n'hésitent pas à s'étiqueter comme sociologues (de l'usage), d'autres mettent en avant le caractère déviant de leurs pratiques et par voie d'extension de leur identité en forgeant ou empruntant d'autres étiquettes : « social scientist », « social designer », « facilitateur d'innovation », « sociologue praticien » ou encore « ingénieur de recherche en sociologie appliquée ». Nous allons voir dans la partie suivante que l'existence de cette nébuleuse d'étiquetages est tout autant liée aux caractéristiques de l'espace référentiel qu'à celles des lieux d'expression dans lequel évoluent les praticiens.

### ***D - La perpétuation de pratiques et savoir-faire : la fragmentation des espaces d'expression***

On peut constater le fait que la littérature convoquée dans ce chapitre est sensiblement différente de celle des deux chapitres précédents. Sur le plan disciplinaire comme sur le plan territorial, les frontières ont été élargies par les références empruntées. Cet élargissement du référentiel analytique coïncide, par jeu de miroirs, avec l'extension de l'espace référentiel dans lequel se situent les praticiens. Ceux-ci ne se bornent pas aux enseignements de la sociologie mais explorent des disciplines telles que les sciences de conception et le design,

---

<sup>144</sup> Retenue le cadre de l'appel à projets « Opération Campus » lancée en 2008 par le Ministère de l'enseignement supérieur et de la recherche, onze partenaires universitaires et scientifiques de l'agglomération grenobloise se sont regroupés sous la dénomination « Grenoble Université de l'Innovation ». Cette structure regroupe institutionnellement un campus à deux têtes : à l'est de la ville, le campus universitaire, tourné vers la recherche fondamentale et l'enseignement supérieur pluridisciplinaire, et à l'ouest, le Polygone scientifique, orienté vers la recherche technologique en liaison avec les entreprises et ayant pour faire de lance Minattec.

la psychologie, la philosophie, les sciences pour l'ingénieur, l'histoire ou encore la créativité pour effectuer leur travail. D'autre part, ils se dégagent de l'ancrage francophone de la « sociologie des usages » et s'alimentent de travaux moins respectueux des règles d'orthodoxie de la discipline. Souvent l'œuvre d'institutions étrangères (scandinaves, anglo-saxonnes), ces travaux rendent compte de bonnes pratiques, d'études de cas, de retours d'expériences ou même de réflexions théoriques concernant les pratiques et savoir-faire de la conception technologique impliquant des sciences sociales. Aussi, l'art comme l'expérience personnelle, les anecdotes, constituent des sources légitimes d'inspiration.

Dès lors, on comprend que cette extension de l'espace référentiel ait pour conséquence la fragmentation de l'inscription dans les espaces d'expression et de publicité de leur travaux. Ces praticiens interviennent tour à tour dans des séminaires de recherche en sciences sociales ou en sciences dites dures, dans des lieux de débat public science-société, comme enseignant dans des formations universitaires, comme formateurs professionnels, pour livrer témoignage auprès de médias, comme représentants d'industriels dans des projets de conception, comme représentants de la « société » dans ces mêmes projets, comme témoins d'une pratique dans des salons professionnels, comme porteurs de projet auprès d'organismes financeurs, et cela indifféremment en France ou à l'étranger.

Cette fragmentation des lieux d'expression participe d'une *horizontalisation* des cycles de crédibilité qui convertissent les productions de sociologues sous forme de reconnaissance. Les différents types de luttes attachées à chacun de ces cycles<sup>145</sup> sont enchevêtrées car société, conseils de recherche, communauté scientifique et laboratoire sont mis sur le même plan du fait des caractéristiques des réseaux dans lequel prend place la *projection d'usage*. Ceux-ci sont des réseaux « structure de projet » (Vinck, 2007). Ils sont composés d'équipes *ad hoc* aux compétences variées et complémentaires avec une répartition et une intégration des tâches entre les équipes. Cette forme d'organisation flexible concentre, le temps de son existence, l'ensemble des problématiques inhérentes aux différents cycles de crédibilité. Cette fragmentation des espaces d'expression a pour effet, non d'intensifier le caractère de la déviance décrite, mais de démultiplier les possibilités d'existence des « entrepreneurs de morale ». En effet, le travail de *projection d'usage* se trouve exposé à la critique d'un nombre d'acteurs élevé, acteurs qui peuvent se poser en défenseurs de l'orthodoxie de territoires visités par les praticiens. Dans le cadre de notre investigation, nous avons retenu une mise en perspective avec les travaux de l'« école

---

<sup>145</sup> Au niveau de la société, la lutte pour la légitimité, au niveau des conseils de recherche, la lutte pour la pertinence de l'activité scientifique, au niveau de la communauté scientifique, la lutte pour le financement et au niveau du laboratoire, la lutte pour la factivité et la scientificité.

française des usages » et avec la méthode CAUTIC™. Nous aurions, dans le même esprit, pu dresser un constat similaire en repensant la carrière d'autres concepts tels que l'« utilisabilité », l'« acceptabilité », la « créativité » ou encore la « conception » pour démontrer le caractère déviant d'une pratique que nous nous attachons à sonder dans le reste de la thèse.

## IV - Conclusion de la partie I

Tableau 3. Synthèse des pratiques et des dynamiques de déviances

		<b>Pratique <i>poïétique</i></b>	<b>Pratique <i>pythique</i></b>	<b>Pratique <i>sibylline</i></b>	
		Quantitativistes	Certains héritiers et tenants de l' « école française des usages »	Gardiens de l'orthodoxie de leur discipline ou pratique relative	<b>Entrepreneurs de morale</b>
		« école française des usages »	Galaxie CAUTIC™	<i>Projection d'usage</i>	<b>Outsiders</b>
<b>Processus de déviance</b>	<b>Transgression</b>	L'usage, construit social	La méthode CAUTIC™	Le travail de projection d'usage	
	<b>Apprentissage social</b>	Interdisciplinarité justifiée par le travail de recherche au concret et ayant un modèle de circulation Régime de production scientifique transitaire	Interdisciplinarité justifiée par la pertinence travail scientifique vis-à-vis de l'objet ou du problème et ayant un modèle fusionnel Régime de production scientifique utilitaire	Interdisciplinarité justifiée par le travail de conquête et ayant un modèle de complémentarité. Régime de production scientifique transversal	
	<b>Désignation publique</b>	« collège invisible »	Méthode « engagée »	Sociologie praticienne tournée vers l'innovation technologique	
	<b>Perpétration de pratiques et savoir-faire</b>	Espace national français ou international francophone Réseau « forum »	Ancrage local (Rhône Alpes) Réseau d'harmonisation des pratiques de recherche	Espace international et fragmenté Réseau structure de projet	

Nous avons, dans cette partie, identifié des carrières idéal-typiques de l' « usage » en associant le concept à des contextes d'utilisation de celui-ci. Cependant, les formes *poïétique*, *pythique* et *sibylline* que nous avons décrites, ne doivent pas amener à la conclusion d'une logique darwinienne de succession de celles-ci. Les transformations observées ne se basent pas sur l'éradication de la carrière précédente. Elles ne relèvent pas, en ce sens, d'une relecture de l'histoire à travers le regard des « vainqueurs ». Car, en

s'armant de la notion de déviance, nous souhaitons profiter de la possibilité de circuler d'un monde à l'autre, d'une « carrière » à l'autre, en étant débarrassés d'intentions normatives et suffisamment équipés pour traquer les liens qui unissent ces mondes de pratiques.

Un retour critique sur notre analyse nous permet de constater qu'elle empreinte une logique d'entonnoir tant quant à l'étendue géographique des lieux investigués qu'à la granularité de l'utilisation du concept d'« usage ». En effet, la pratique de l'« école française des usage » est ancrée dans un territoire national, sinon francophone, et les pratiques ne sont qu'investiguées d'un point de vue généralisant. La pratique *pythique* de l'usage nous fait descendre d'une échelle géographique puisqu'elle s'inscrit d'abord sur le territoire isérois du fait de son analyse par le biais d'une méthode idoine dont le succès fut d'abord local. Enfin, la pratique *sibylline* de l'usage s'inscrit en un lieu restreint, le CEA et son environnement, et elle fait l'objet, dans les chapitres suivants, d'investigations poussées qui forme le canevas empirique de notre travail de thèse. Nous constaterons également que cet effet de *zoom avant* sur les lieux et les pratiques investiguées est contrebalancé par l'élargissement des réseaux au sein desquels s'inscrivent les communautés de recherche abordées. Cet élargissement se traduit à la fois sur le plan d'une intensification des collaborations avec d'autres communautés que les communautés académiques, mais aussi par l'internationalisation des lieux d'expression et de communication de travail scientifique. Cet effet de *travelling compensate*<sup>146</sup> permet de comprendre le recours, dans cette thèse, à des sources disciplinaires variées ; recours qui participe d'une forme de déformation professionnelle due au temps passé au sein d'équipes pratiquant l'usage de manière oraculaire. Il permet également de rendre compte des contraintes inhérentes au travail de thèse qui, du fait du temps disponible et de la limitation des terrains investiguables, peuvent s'avérer en bout de compte riches en surprises : descendre d'échelle peut permettre de constater des phénomènes d'élargissement.

Enfin, par souci d'honnêteté, il importe d'appliquer à notre analyse le même traitement que celui que nous avons porté à l'usage comme objet scientifique. En décrivant les différentes carrières de l'usage et de ces pratiques, nous avons souhaité rendre plus tangibles les réseaux qui se constituent autour de l'idée que ses membres se font des rapports entre science et société. Notre travail, en tant qu'entreprise à prétention scientifique, ne s'effectue pas dans une objectivité absolue. En traitant de l'usage et des ramifications de ses réseaux de pratiques, nous affirmons l'intérêt à se pencher attentivement sur les remous

---

<sup>146</sup> Mouvement de caméra complexe, associant un zoom avant sur le sujet principal et un travelling arrière sur l'arrière-plan, de telle sorte que le sujet principal reste cadré de la même manière, seul le décor changeant de perspective.

traversés par la sociologie, comme science et comme pratique sociales. Ce faisant, nous portons implicitement la revendication que la médiatisation de la sociologie ou sa diffusion hors des cercles scientifiques autorisés, loin de porter atteinte à la probité de cette science, contribue à sa publicité et donc à sa pérennité dans la cité (Lemieux, 2010). Nous ne nions pas que l'information scientifique soit alors menacée par un fort degré de déperdition à mesure qu'elle s'éloigne de ses sources de production, ni que les causes de mobilisation de la sociologie dérogent à l'éthos scientifique. Cependant, plutôt que d'avoir concentré nos efforts sur la construction d'une éthique universelle de la science et de ses usages – ce qui n'est pas sans intérêt d'un point de vue philosophique, nous avons souhaité comprendre comment les intérêts propres et les horizons d'attente d'*outsiders* pouvaient devenir les moteurs de formes locales de dialogue entre science et société. C'est à certaines de ces modalités de dialogue que nous allons nous intéresser dans les deux parties qui constituent notre enquête empirique.

## **Partie 2. La projection d'usage, genèse d'une écologie socio-technique**

*« Little flightless metal birds  
High above in limbless tree  
Echoes from their tiny box  
Ring out into the atmosphere  
Creating beauty inadvertently*

*It was a technological feat*

*This little bird*

*Wading through the market's waste  
We locked eyes felt our loneliness abate  
True desire showed its face, but only momentarily*

*Grey cascades in foreign waves  
Wash the day away”*

*TV on the Radio, “Wash the Day Away”, in the album Return to Cookie Mountain, Interscope Records*



Notre étude empirique est fondée sur un projet de recherche industrielle porté par le CEA-LETI. Son axe thématique principal est la sécurisation des télécommunications et des réseaux. Le projet COPRIM (COnтактless PRIVacy Manager) est un projet de recherche industrielle multipartenaire de trois ans (2008-2011) bénéficiant du soutien de l'Agence Nationale de la Recherche (ANR). Porté par le CEA-LETI, le projet associe trois autres partenaires : un laboratoire de cryptologie (PRISME/UVSQ), un industriel spécialiste des cartes à puces sans contact (Inside Contactless) ainsi qu'une équipe de sciences sociales (Umanlab/UPMF). Il a pour principal objectif la sécurisation des transactions de données confidentielles entre dispositifs de communication sans contact en champ proche (NFC<sup>147</sup>). En effet, la technologie NFC permet de relier avec des protocoles sécurisés les objets du quotidien. Une « puce » NFC intégrée dans ces objets (ordinateurs, téléphones, cartes à puce, télévisions, tablettes, imprimantes, réfrigérateurs, etc.) permet l'identification ou le transfert de données et ouvre à de nouveaux modes de communication entre objets et entre personnes détentrices de ces objets. En se basant sur les projections annonçant le couplage généralisé de cette technologie avec le téléphone portable et ses usages liés (le téléphone pourra jouer les rôles de badge d'accès, de porte-monnaie électroniques, de carte de fidélité, de carte de crédit ou encore de carte de transport – voir Figure 6), le projet induit l'émergence de problématiques portant sur la sécurisation des données échangées ainsi que sur le rôle dévolu à l'utilisateur dans la gestion de ses données personnelles liées à l'utilisation de son mobile.

*Figure 6. Exemples d'usage d'un téléphone NFC*



La finalité du projet a été déclinée en quatre objectifs de majeurs :

<sup>147</sup> NFC est le sigle retenu pour « Near Field Communication », c'est-à-dire pour les produits fonctionnant en couplage inductif, et donc à courte portée contrairement au sans fil. Nous reviendrons sur le rôle de cette technologie mais nous pouvons dès à présent noter que ce standard est en cours de déploiement sur l'ensemble des téléphones portables.

- « proposer des primitives de solutions technico-économiques de protection de la vie privée des systèmes de type NFC
- (re)donner confiance à l'utilisateur dans les produits sans contact (NFC)
- établir un business model de diffusion des primitives de protection de la vie privée
- valider sur des scénarios pertinents ces primitives de protection de la vie privée. »<sup>148</sup>

Dans cette partie, nous étudierons dans un premier temps l'organisation globale du projet en y analysant le processus de stabilisation de l'innovation. Nous verrons que la projection d'usage consiste en l'élaboration d'une *écologie socio-technique* obtenue par le rapprochement d'un cadre de fonctionnement et d'un cadre d'usage et la mise à l'épreuve de la projection (V). Nous nous intéresserons ensuite plus spécifiquement à la projection d'usage en se concentrant sur l'une de ces modalités d'expression : le scénario. Nous aborderons ainsi les différentes formes d'usage du scénario dans le champ de la conception afin d'en définir les contours pluriels (VI) avant d'en justifier l'étude par sa qualité d'« *objet intermédiaire de conception* » (Jeantet, 1998 p. 325). Nous expliciterons ensuite notre méthode d'investigation, l'observation participante, comme moyen privilégié d'accès au terrain et à ses mouvements (VII). Nous concluons cette partie en explicitant l'ancrage de notre réflexion sur le concept d'« *objet-frontière* » (Griesemer & Star, 1989).

---

<sup>148</sup> Cet extrait est issu de l'annexe technique du projet. Pour ce chapitre, chaque élément qui en sera extrait est mis entre guillemet sans que la source ne soit précisée.

## V - Le projection d'une écologie socio-technique stable

Pour atteindre son objectif de sécurisation des transactions de données confidentielles entre dispositifs de communication sans contact en champ proche (NFC), le projet COPRIM est organisé en séquences de travail visant à produire un faisceau d'indices démontrant la réussite de l'opération menée. Il est divisé en cinq lots (« workpackages » ou WP), le dernier étant dévolu au management du projet. Les quatre premiers lots sont programmés sur un processus en trois étapes :

- la première phase (première année) vise à « l'analyse des menaces principales qui pèsent sur la « Privacy » de l'utilisateur de dispositifs sans contact ». Elle correspond au premier lot (WP1),
- la deuxième phase (deuxième année) est une phase de conception et de validation des plateformes de développement technologique (WP2 et WP3),
- La troisième phase (troisième année) correspond à la validation de la finalité du projet à l'aide de l'évaluation du démonstrateur conçu (WP 4).

Figure 7. Diagramme de GANTT de COPRIM

	Year 1					Year 2					Year 3				
<b>WP1</b>															
T1.1 Personal data and privacy use cases															
T1.2 CPM and threats analysis															
T1.3 CPM specifications															
<b>WP2</b>															
T2.1 Design of protection at physical level															
T2.2 Design of protection at protocol level															
T2.3 Cross layer design															
<b>WP3</b>															
T3.1 Demonstrator specifications															
T3.2 Demonstrator development															
T3.3 Demonstrator test and validation															
<b>WP4</b>															
T4.1 Use case security demonstration															
T4.2 Use case privacy validation															
<b>WP5</b>															
T5.1 Project coordination															
T5.2 Results dissemination															

A l'issue du projet, plusieurs éléments de preuve ont été produits et l'ensemble de ceux-ci constitue un faisceau d'indices accréditant le caractère innovant des solutions de sécurisation des transactions de données confidentielles entre dispositifs de communications NFC développées :

- plusieurs démonstrateurs fonctionnels<sup>149</sup> ont été développés et intégrés dans divers modèles de téléphone mobile NFC. Certains de ces démonstrateurs intègrent notamment des protocoles sécurisés mis en œuvre par l'UVSQ. Ces démonstrateurs sont également des supports de communication à l'intention des partenaires du CEA/LETI et de Inside Contactless,
- le CEA-LETI a déposé 3 brevets internationaux concernant la sécurité des communications sans contact,
- L'UVSQ a développé et mis en œuvre des protocoles sécurisés qui sont valorisés aussi au travers de certains démonstrateurs d'Inside Secure,
- En termes de valorisation scientifique, le travail a donné lieu à six communications internationales avec actes, quatre communications nationales avec actes ainsi que deux articles d'ouvrages.

L'émergence de l'innovation, finalement stabilisée par le faisceau d'indices, a été organisée en orientant l'activité vers la construction d'un « *cadre de référence sociotechnique* » (Flichy, 2003). L'équipe-projet s'est ainsi doté d'un « *cadre de fonctionnement* » circonscrit et d'un « *cadre d'usage* » projeté pour les faire converger afin de se rapprocher le plus possible d'une stabilisation de l'innovation en construction. Le résultat de ces opérations est cristallisé par une *écologie socio-technique* cristallisée dans la matière du scénario d'usage.

### ***A - Positionner le projet dans un cadre de fonctionnement circonscrit***

Les phases 1 et 2 du projet sont organisées comme un processus de définition du « *cadre de fonctionnement* » (Flichy, 2003) de la solution de sécurisation :

---

<sup>149</sup> Pour des raisons de confidentialité, nous ne pouvons pas reproduire le démonstrateur par une photo.

*« Le cadre de fonctionnement définit un ensemble de savoirs et de savoir-faire qui sont mobilisés ou mobilisables dans l'activité technique. Ce cadre est non seulement celui des concepteurs d'un artefact technique, mais il est aussi celui des constructeurs, celui des réparateurs et également celui des usagers. » (Flichy, 2003 p. 124).*

En tant que concepteurs, l'équipe va positionner son projet dans un cadre de fonctionnement spécifique en recensant les savoirs et savoir-faire mobilisables (phase 1), puis en mobilisant les savoirs et savoir-faire considérés comme les plus pertinents au vue de leur objectifs et selon des critères qu'ils ont déterminés (phase 2). Ce processus de stabilisation du cadre de fonctionnement aboutit à la création d'un démonstrateur, *« traduction physique d'un système intellectuel. »* (Flichy, 2003 p. 211).

La phase 1 (*« analyse des menaces principales qui pèsent sur la « Privacy » de l'utilisateur de dispositifs sans contact »*) donne ainsi lieu au recensement de savoirs et savoir-faire hétéroclites mobilisés autour de la notion de *« Privacy<sup>150</sup> »*. Ce faisant, l'équipe-projet procède à plusieurs opérations d'inscription de l'objet d'innovation dans une historicité à plusieurs niveaux :

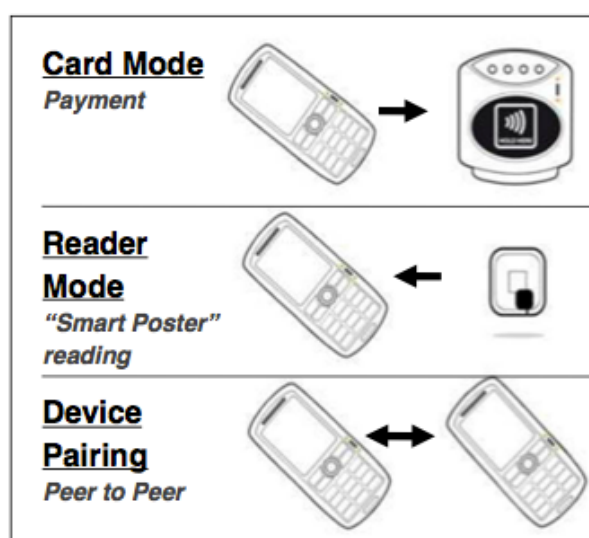
- En choisissant de s'intéresser aux transactions NFC, l'équipe-projet positionne son cadre de fonctionnement dans la galaxie de standards de normalisation des transactions entre dispositifs de communication NFC (ECMA et ISO 18092, ISO 14443, ISO 15693 et Felica). Cette inscription permet à l'équipe-projet de définir la liste des menaces portant sur les transactions entre dispositifs NFC (voir Tableau 4) à partir des trois modalités de fonctionnement existantes (voir Figure 8). La solution COPRIM est envisagée comme la mutation de ce cadre préexistant par sa sécurisation.
- Sur un plan plus large, on peut considérer que la solution est sensée être compatible avec des systèmes techniques de taille différentes, systèmes interagissant sur le modèle des poupées gigognes. Le NFC est intégré dans un smartphone, lui-même intégré dans un réseau d'ondes plurielles, elles-mêmes interagissant avec des écosystème d'objets connectés (ordinateur, terminaux de paiement, terminaux de validation de titres de transport, terminaux d'identification, etc.), eux-mêmes reliés à des infrastructures diverses (infrastructures réseaux, infrastructure de transport, lieux de commerces, etc.), elles-mêmes structurant des champs politiques, économiques et

---

<sup>150</sup> Nous développons plus avant dans le chapitre X les implications de la réunion de ces éléments disparates sous la bannière de cette notion polysémique.

sociaux plus larges (réseaux de grande distribution, réseaux de transport, réseau de salles de spectacles, etc.). La liste est sans fin mais en définir des exemples permet de comprendre que le processus de définition du cadre de fonctionnement nécessite, d'une part, l'inscription dans un cadre de fonctionnement précédent, d'autre part, et pour assurer sa propre stabilisation, la circonscription des objectifs du projet à une liste de menaces réduites.

*Figure 8. Modes de fonctionnement du NFC*



La phase 2 du projet, notamment le WP2<sup>151</sup> (la conception distincte de solutions de protections au niveau protocolaire et la conception de solutions de protections au niveau physique), a pu débuter dès le lancement du projet car les activités de conception du CEA/LETI, au niveau de la couche physique, et de l'UVSQ, au niveau de la couche protocolaire, avaient déjà été engagés avant le lancement du projet. En effet, l'inscription de la solution dans l'écosystème du NFC avait permis aux deux acteurs d'amorcer de manière autonome des recherches de solution de protection avant le début du projet, travaux qu'ils ont ainsi pu poursuivre et consolider avant d'entamer la phase de conception d'une solution joignant les couches physique et protocolaire (T2.3).

<sup>151</sup> Nous verrons plus tard que le WP3, qui appartient également à la phase 2, entre dans la construction du cadre de référence socio-technique.

*Tableau 4. Liste des menaces sur la sécurité des transactions NFC*

Type d'attaque	Objectifs de l'attaque
Eavesdropping (littéralement, le fait d'écouter aux portes)	Une tierce personne intercepte les échanges d'informations entre deux dispositifs NFC. Cette attaque permet donc de récupérer des données utiles en soi ou de se servir de ces données pour mener une autre attaque.
Skimming (littéralement, le fait de frôler quelqu'un ou quelque chose)	Un tiers utilise un dispositif NFC pour lire les informations présentes sur un autre dispositif, sans consentement du propriétaire de ce dernier.
Relay attack (littéralement, l'attaque en relai)	C'est une variante du skimming. Un tiers lien est établi entre deux dispositifs NFC en contact, qui permet de récupérer les données échangées sans que les deux utilisateurs ne s'en aperçoivent.
Man-in-the-middle (littéralement, l'homme au milieu)	Un tiers lien est établi entre deux dispositifs NFC en contact, qui permet de modifier la nature des données échangées sans que les deux utilisateurs ne s'en aperçoivent.
Malicious software attack (littéralement, attaque malicieuse de logiciel) Phishing (littéralement, le hameçonnage)	Cette menace consiste à « contaminer » le logiciel du téléphone par un virus, un cheval de Troie ou un vers afin d'en prendre le contrôle ou d'obtenir, à l'insu de l'utilisateur trompé, des informations confidentielles.
Spamming (le fait d'envoyer des spams)	Cette menace décrit le fait d'envoyer à l'utilisateur non consentant des informations ou des liens vers des plateformes, au mieux publicitaires, au pire, ouvrant la voie à du phishing ou à la contamination du mobile.

Avant que ne soit entamée la dernière phase de stabilisation du cadre de fonctionnement, l'équipe-projet a, comme annoncé précédemment, sélectionné un nombre restreint d'attaques que le dispositif de sécurisation se devait de contrecarrer : les attaques en relais et l'eavesdropping. La stabilisation définitive du cadre de fonctionnement est matérialisée par

la réalisation de plusieurs démonstrateurs (voir Figure 9). Comme le souligne Patrice Flichy, le démonstrateur est l'instanciation du processus de conception durant lequel le concept est réifié dans une boîte noire : *« Par la suite, les différents éléments vont converger dans un objet technique concret, plus compact. Chaque élément est maintenant intégré dans un système qui a acquis sa propre cohérence. L'objet devient une « boîte noire » qui fonctionne, pour l'utilisateur profane mais aussi pour l'ingénieur, sans que l'on ait besoin de se remémorer l'articulation des différents sous-ensembles. Le cadre de fonctionnement a trouvé sa stabilité. On assiste alors à ce phénomène de verrouillage technologique »* (Flichy, 2003 p. 211).

*Figure 9. Présentation d'un démonstrateur telle que symbolisée dans la présentation finale à l'ANR. le 8 mars 2012*



### ***B - Positionner le projet dans un cadre d'usage projeté***

En parallèle de l'établissement de ce cadre de fonctionnement, le projet a inscrit dans son organisation la création d'un cadre d'usage. Le cadre d'usage s'élabore également au cours d'un processus complexe mais renvoie aux imaginaires, représentations, perceptions et arts de faire d'une population confrontée à l'utilisation d'un dispositif technique (Flichy, 2003). Devant l'impossibilité d'interroger l'inexistant, c'est-à-dire l'usage effectif d'une technologie en conception, l'équipe-projet a développé deux axes de construction du cadre d'usage :

- un axe de justification qui pose la prise en compte du cadre d'usage durant le processus de conception comme condition *sine qua non* de la réussite de l'innovation



- un axe de création qui définit les modalités d'élaboration du cadre d'usage en absence de possibilités de rencontre entre l'utilisateur et la technologie.

D'abord, la mobilisation d'un cadre d'usage est justifiée par la nécessité de sa prise en compte pour attester du caractère innovant de la solution déployée. En effet, le projet n'est pas défini comme devant accoucher d'une preuve de concept de fonctionnement de la solution. Il est plutôt envisagé comme un projet aboutissant à la conception d'une innovation, c'est-à-dire d'une invention diffusable au sein d'un terrain social et économique existant. Le recours au cadre d'usage est présenté comme un élément fondamental du faisceau d'indices à produire par la démonstration que la sécurisation des transactions NFC répond à un besoin de « *Protection des informations personnelles sur les objets nomades de type mobile NFC* » :

*« L'accroissement des fonctions de connectivité embarquées sur les objets portables de type téléphone mobile augmente les risques d'accès aux données personnelles de l'utilisateur par des acteurs malveillants. La convivialité de ces objets et leur utilisation quotidienne et fréquente nécessitent de disposer de fonctions de communications sécurisées. Ces communications sécurisées doivent inspirer confiance aux utilisateurs qu'ils soient propriétaires de l'objet nomade ou fournisseurs de services à distance.*

*La contribution du dispositif COPRIM à l'établissement de la confiance chez l'utilisateur repose notamment sur deux éléments complémentaires : la technologie déployée pour protéger les utilisateurs et l'acceptabilité par le consommateur des solutions techniques mises en oeuvre. C'est pourquoi un partenariat multidisciplinaire intégrant des compétences techniques du domaine des technologies de l'information et de la sociologie des usages a été mis en place. Il se propose de fournir des solutions techniques validées vis-à-vis de leur acceptation par l'utilisateur d'objets portables de type mobile NFC. »*

La confiance est donc le besoin identifié par l'équipe-projet qui se donne comme objectif l'établissement de celle-ci chez l'utilisateur, objectif dont l'évaluation repose sur l'acceptabilité de la solution mise en oeuvre. Ces deux composantes du processus de construction du cadre d'usage vont être développées en deux lieux que Patrice Flichy<sup>152</sup> considère comme des lieux de médiation importants dans l'élaboration du cadre d'usage :

<sup>152</sup> « Dans ce jeu d'élaboration successive du cadre d'usage, il existe deux lieux de médiation importants, l'équipe-projet et les premiers sites où l'artefact est utilisé. (...) Dans cette équipe, la question du cadre d'usage est largement débattue, surtout au début, dans la période où il faut définir les grandes fonctionnalités, et plus tard, lorsque le produit va sortir sur le marché. Au sein du groupe, chacun des participants arrive avec sa représentation des usages potentiels, sa connaissance des modes de vie. Et de cette confrontation naît généralement un premier cadre d'usage » (Flichy, 2003, p.217)

l'équipe-projet et les premiers sites d'utilisations de l'objet.

L'équipe-projet va donc mobiliser, toujours autour de la notion de « *Privacy* », et parallèlement à l'élaboration du cadre de fonctionnement, un premier cadre d'usage nécessaire à la définition des spécifications techniques de la solution de protection (état de l'art, T1.3). Ce cadre a fait l'objet de discussions animées et résulte de négociations entre plusieurs représentations de l'usage portées par les différents acteurs de l'équipe-projet<sup>153</sup>. Il est d'abord matérialisé dans l'état de l'art sur la notion de « *Privacy* » en sciences sociales qui atteste de cette volonté d'identifier les grandes représentations et perceptions des notions de vie privée, de sécurité et de protection de données privées en dehors et dans le cadre de l'usage des technologies de l'information et de la communication. Il continuera de se définir à travers la rédaction des scénarios d'usage (scénarisation, T1.1) qui vont s'appuyer sur les ressorts de la fiction (voir Partie III) pour le consolider. La notion de confiance a été positionnée comme le pivot de construction de ce premier cadre d'usage.

Dépourvu de premier site d'utilisation de l'objet, l'équipe-projet a consolidé, lors de la troisième année du projet, la stabilité de ce premier cadre d'usage en le mobilisant comme un support de « test d'acceptabilité », dont nous parlons plus en détail dans la partie suivante. Néanmoins, au-delà du test en lui-même, le fait même de mobiliser cet objet en dehors du lieu de sa production, achève sa stabilisation en parant celui-ci des qualités du « *mobile immuable*<sup>154</sup> » (Latour, 1987) et en usant d'une représentation figée, les scénarios d'usage. Ce faisant, le cadre d'usage est mobilisé comme une convention (*a minima* celle de l'équipe-projet), c'est à dire comme un objet stabilisé qui ne fait plus apparaître de dispute ou de discussion sur sa composition. Durant ces tests, le cadre d'usage projeté est utilisé comme un objet stable et normé, s'apparentant à « *une norme sociale ou à une convention* » (Flichy, 2003, p.218)

---

<sup>153</sup> (voir Partie IV)

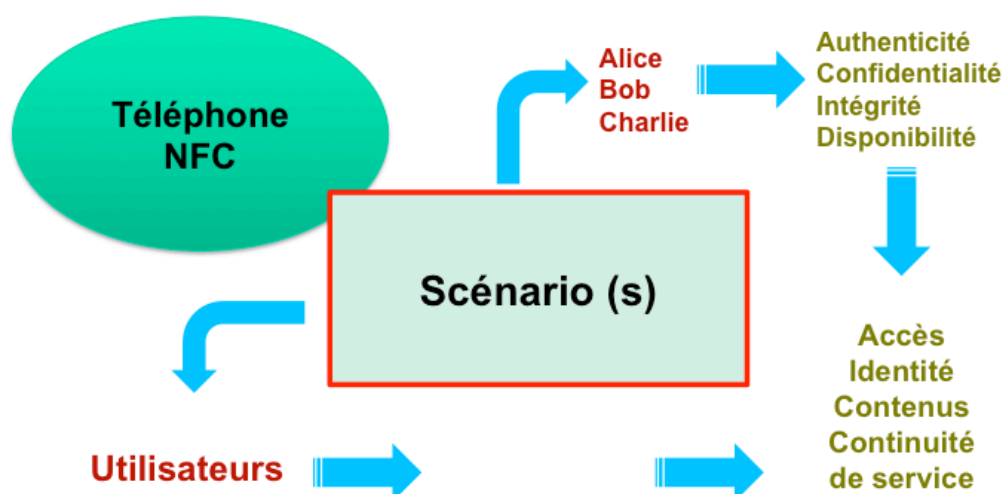
<sup>154</sup> Ils ont pour propriété d'être aussi mobiles qu'immuables, présentables, lisibles et combinables avec d'autres objets. A l'exemple de la carte géographique, elles conservent leurs formes (immuables) tandis qu'elles circulent dans le temps et l'espace (mobile). « [...] il faut faire venir le monde en certains points qui deviennent alors des centres ou des points de passage obligé. Très bien, mais sous quelle forme faire venir le monde pour que, d'une part, ce qui est loin, distant et périssable, s'y trouve assemblé, et que, d'autre part, le centre ainsi constitué ne soit pas un formidable embouteillage ? Il faut inventer des dispositifs qui mobilisent les objets du monde, maintiennent leur forme et puissent s'inspecter du regard. Il faut surtout que toutes ces formes puissent se combiner à loisir et se retravailler de telle sorte que celui qui les accumule dispose d'un surcroît de pouvoir. Alors, et alors seulement, certains points deviennent des centres capables de dominer sur une grande échelle. Dans la suite des recherches, je ne parlerai plus des lieux où se cumulent les mobiles immuables que comme des centres de calcul, sans plus m'occuper de savoir à quels domaines ces calculs ressortissent. » (Latour, 2006 p. 33-34).

### ***C - Consolider la projection d'une écologie socio-technique***

La logique du projet tend vers la mise en œuvre d'un « *cadre de référence socio-technique* », c'est à dire d'une entité nouvelle et stable, véritable « *alliage* » mêlant indifféremment cadre de fonctionnement et cadre d'usage jusqu'à devenir, pour l'ensemble de la chaîne d'acteurs concernés (concepteurs, fabricants, vendeurs, clients, utilisateurs) une boîte noire (Flichy, 2003).

Devant l'impossibilité de parvenir à cette fin, l'équipe-projet s'inscrit dans une dynamique asymptotique : à défaut de pouvoir obtenir un véritable cadre de référence socio-technique, elle jalonne le processus d'épreuves de validation témoignant de la stabilisation et de l'alliage progressifs du cadre de fonctionnement et du cadre d'usage. Pour ce faire, l'équipe soumet le processus à deux « *tests prospectifs* » pour soumettre la technologie et son usage à l'épreuve d'un usage généralisé (Pinch, 1993).

Dans un premier temps, la définition des spécifications du démonstrateur procède de la réunion d'enjeux propres au cadre de fonctionnement et d'enjeux inhérents au cadre d'usage par leur assimilation dans les scénarios. Les scénarios, adossés au cadre de fonctionnement du téléphone NFC sont constitués comme des réponses aux enjeux « techniques » et « sociétaux » identifiés par l'équipe-projet. Ils constituent une première approche d'un cadre de référence socio-technique en ce qu'ils tentent la concentration dans un même objet du cadre de fonctionnement et du cadre d'usage (voir Figure 10).



*Figure 10. Schéma présent dans la présentation du 04/09/2009 devant l'équipe projet par Umanlab et fréquemment réutilisé dans la documentation à destination de l'ANR*

Figure 11. Guide d'entretien CAUTIC 1/2

<p>1. Confrontation to the know how of the users  <b>1.1/ The technical operating principle looks immediately understandable</b>  Exploration du critère en deux temps:  Temps 1 – Juste avant présentation du concept :  <b>Grand public</b> : Jusqu'ici est-ce que ça va ? Vous comprenez ? Qu'est-ce que ça vous inspire ? Avez-vous une réaction spontanée par rapport à ce concept ?  <b>Expert ou Professionnel</b> : Jusqu'ici est-ce que ça vous parle ? Qu'est-ce que ça vous inspire ? Avez-vous une réaction spontanée par rapport à ce concept ?</p> <p>Temps 2 – Juste après présentation complète (scénarios inclus) :  <b>Grand public + Expert</b> - Avez des réactions ou des questions suite à la présentation du concept et des scénarios d'utilisation ? Est-ce qu'il y a des zones d'ombre? Voulez-vous que je revienne sur un point précis? Comprenez-vous à quoi ça sert ? Sauriez-vous l'utiliser ?</p> <p><b>1.2/ The new technique is supported by a pre-existing usual technique</b>  <b>Grand public</b> – Est-ce que le système [COPRIM] vous rappelle quelque-chose que vous utilisez, ou une autre technique? Pouvez-vous le comparer à un système existant ? Relances  Est-ce que ça apporte quelque chose de plus par rapport à ces systèmes ou techniques que vous utilisez ?</p> <p><b>1.3/ For the whole of the technical functionalities offered it is clear for the user that he can easily and simply use the one(s) he is interested in</b>  Parmi les 5 cinq fonctionnalités clés/structurantes du concept qu'on vous a présentées est-ce que vous en avez identifié une ou plusieurs qui soient plus particulièrement intéressantes ? Relances. Au besoin lister à nouveau les 5 fonctions.</p> <p><b>1.4/ The use of the technique is not only a social distinction issue for the user. He considers that this new technique could be of common use</b></p>	<p>Imaginez-vous le système [COPRIM] comme un outil d'usage courant, ordinaire ou bien ponctuel et lié à des situations particulières ?  Relance  Est-ce que c'est vraiment utile ? ou est-ce que ça va le devenir ? est-ce que c'est un gadget ?</p> <p><b>2. Confrontation with the usual users' practices 2.1/ The new practices complete the existing practices without competing immediately with them</b></p> <p>Est-ce que vous avez déjà des activités d'échange d'information en mobilité, sans fil avec votre ordinateur ou votre téléphone par exemple ?  Relance</p> <p><b>2.2/ The comparison to the existing practices validates (makes credible) the new practices offered</b></p> <p>Est-ce que les pratiques/activités dont vous venez de nous parler vous laissent imaginer que vous puissiez avoir besoin d'un tel système [COPRIM] un jour ?  Relances  <b>Grand Public</b>  Demain vous avez un téléphone NFC dont vous vous servez régulièrement. Ce qui vous a été montré dans le(s) scénario(s) : le feriez vous sans COPRIM ?  Relances  <b>Pro/Expert</b>  Demain vos clients/partenaires utilisent les téléphones NFC... Proposeriez-vous des services/applications comme ceux présentés dans les scénarios? Proposeriez-vous à vos clients des applications/services comme ceux des scénarios sans un système comme COPRIM ?</p> <p><b>2.3/ At least one particularly annoying problem in the previous practices is solved for each user type in the new practices</b></p> <p>Selon vous est-ce que le système [COPRIM] résoudrait un ou des problèmes ?</p> <p><b>2.4/ The user progressively builds a specific organization of his new practices.</b></p>	<p>Est-ce que vous imaginez utiliser des transactions « sans contact » de plus en plus régulièrement ? (pas forcément avec un téléphone mais aussi des cartes).</p> <p>Est-ce qu'il serait intéressant d'utiliser le système [COPRIM] pour ajouter un niveau de sécurité dans les transactions entre vos cartes sans contact existantes et les lecteurs ? (c'est-à-dire sans remplacer la carte par le téléphone). Relances</p> <p><b>3. Confrontation with the user's social/professional identity</b></p> <p><b>3.1/ With the product/service the user can personally act on/play with his social and/or professional role</b></p> <p>Dans un environnement technique « sans contact » (supposons que l'on utilise des cartes et téléphones dit NFC demain), est-ce que vous sentez en sécurité ? Est-ce que le système [COPRIM] vous fait sentir plus en sécurité ?</p> <p>Faites-vous confiance au système [COPRIM] ? Vos informations personnelles, est-ce que c'est quelque chose qui vous préoccupe ?</p> <p>Est-ce que vous délégueriez la protection de vos informations personnelles, des transactions d'informations au système [COPRIM] ?</p> <p>Imaginez-vous utiliser le système [COPRIM] de manière transparente ou bien au contraire contrôler au maximum ses activités ? Avoir une visibilité permanente sur les activités qu'il contrôle ? Relances Comment diffusez-vous vos informations personnelles sur les réseaux sociaux (FaceBook et autres) ?  <b>Expert/Pro</b>: Est-ce que le «sans contact» associé au système [COPRIM] vous permettrait de mieux faire votre travail ?</p> <p><b>3.2/ The product/service is compatible with the cultural values of the various types of users</b></p> <p>Est-ce que l'utilisation de ce système [COPRIM] est cohérente avec vos principes ? Relances</p>
--	---	--

Figure 12. Guide d'entretien Cautic 2/2

<p>Compatible avec vos valeurs, croyances, règles personnelles, culture? Est-ce que ce système est bon ou mauvais?</p> <p><b>3.3/ The product/service provokes an imaginary of appropriation</b></p> <p>Si c'était un animal/ personnage célèbre? Pourquoi?</p> <p><b>3.4/ The product/service leaves the possibility of imagining extensions of use</b></p> <p>Imaginez-vous des applications du système [COPRIM] complètement différentes, des scénarios complètement différents ? Relance Imaginez-vous des détournements d'usage?</p> <p><b>4 Confrontation with the structures and the overall development of the user's social and professional environment</b></p> <p><b>4.1/ The availability of the product/ services is seen as realistic regarding society values and market trends</b></p> <p>Ce système [COPRIM], est-ce que vous y croyez? Quel horizon temporel (court/moyen/long termes) Relances</p> <p><b>4.2a/ The innovation is considered by the professional/industrial user as adapted to the supplier/client relationships.</b>  <b>Pro</b> Est-ce que le système [COPRIM] est compatible avec votre réseau de clients, fournisseurs ou partenaires en général ? Relance Est-ce que ce système n'est pas en concurrence ou conflictuel avec d'autres systèmes ou options/solutions envisagées par votre réseau ?</p> <p><b>4.2b/ Le produit est perçu comme adapté à l'évolution des formes de sociabilité</b></p> <p>Est-ce que vous imaginez le de personnes ou d'amis ou avec lesquelles vous pourriez utiliser cet appareil ? (Pensez-vous que vous et vos amis allez utiliser ce système ?). Relance</p>	<p>Est-ce que techniquement c'est possible? Est-ce que c'est réaliste, pas trop futuriste  Est-ce que ce serait faisable d'un point de vue business/ économique ?(ça s'intégrerait dans votre offre de produits/ services)</p> <p>Est-ce que ce serait normal dans votre milieu social d'utiliser ce système ?</p> <p><b>4.3a/ The innovation is considered by the professional/industrial user as adapted to his role in the company and/or in the sector/chain he is involved</b>  <b>Pro</b> Serait-il logique dans votre entreprise d'exploiter ce de système ?</p> <p>Verriez-vous l'utilisation de ce système comme un avantage stratégique ou compétitif pour votre entreprise ? Relance</p> <p>Est-ce que votre entreprise pourrait être « pionnière » dans l'utilisation de ce système ou au contraire attendrait plutôt que d'autres testent avant vous ?</p> <p><b>4.3b/ Le produit est perçu comme adapté à l'évolution des formes relations familiales</b></p> <p>Pensez-vous que vous et les membres de votre famille (couple/parents/enfant) vont utiliser cet appareil? (Pensez-vous que vous et vos amis allez utiliser ce système ?) Relance Est-ce que vous équiperiez votre enfant d'un téléphone NFC (« sans contact ») sans COPRIM/avec COPRIM ?</p> <p><b>4.4a/ The new system is considered as adapted to the user's organisation/company and its capacity to evolve</b></p> <p>Au cas de réponse non apportée par critère 4.2a et 4.3a : est-ce que ce système [COPRIM] changerait quelque chose dans vos manières de travailler ?</p> <p><b>4.4b/ Le produit est perçu comme adapté à l'évolution des manières de vivre et d'habiter (implication des individus dans l'information et la culture)</b></p> <p>Est-ce que cela va changer quelque chose dans vos relations avec les</p>	<p>autres (amis/ famille) ? Dans vos manières de vivre en famille ?</p> <p>Fin</p> <p>On a terminé, est-ce que vous avez quelque chose à ajouter ? Pensez-vous à une question que je ne vous ai pas posée ?</p>
---	---	---



Dans un deuxième temps, les indices de l'effectivité d'un alliage des cadres sont recherchés dans l'organisation d'un test d'acceptabilité de la solution développée (T4.2). Onze individus ont été interviewés dans un questionnaire de 30 à 45 minutes selon la méthodologie CAUTIC<sup>TM</sup> afin d'évaluer la « valeur d'usage » de la solution COPRIM<sup>155</sup>. Le guide d'entretien est structuré en quatre parties qui sondent l'assimilation de l'innovation aux savoir-faire techniques familiers de l'utilisateur, l'intégration de l'innovation au sein des pratiques courantes, l'appropriation de l'innovation en fonction de l'identité de l'utilisateur et l'adaptation de l'innovation à l'environnement social et/ou professionnel de l'utilisateur. Plus spécifiquement, les thèmes abordés ont couvert les questions de traçabilité de l'échange de données, les possibilités de contrôle et de paramétrage du dispositif par l'utilisateur, les solutions de protection contre les attaques éventuelles, l'information et le retour d'information à l'utilisateur et l'identification de l'utilisateur.

L'objectif, pour l'équipe-projet, était d'identifier les éléments qui pouvaient, dans les scénarios, être considérés comme freins (rouge), conditions (jaune) ou incitateurs à l'usage (vert) du dispositif CPM en particulier et du NFC dans une plus large mesure. Les résultats de l'étude menée (voir Figure 13) laisse apparaître un consentement généralisé de la part de l'échantillon malgré quelques points problématiques que sont les risques inhérents à la traçabilité et ceux propres aux interactions homme-machine non désirées. Les conclusions de l'étude font porter le poids de la responsabilité et de la sécurisation des données échangées autant sur le dispositif technique que sur l'ensemble des acteurs engagés à travers l'usage de ces dispositifs (opérateurs téléphoniques, compagnies de transport, banques). Des recommandations pour les étapes suivantes de la conception sont basées sur ces résultats. Elles prônent notamment l'obligation d'améliorer et de rendre disponible à l'usage le contrôle de la traçabilité de la circulation des données.

En soumettant sa projection d'usage au jugement d'utilisateurs potentiels et en tirant l'approbation de ceux-ci, l'équipe-projet a pu compléter son faisceau d'indices lui permettant, non seulement de consolider et stabiliser sa projection d'usage, mais aussi de l'inscrire dans une dynamique future d'invention à forte potentialité innovante. Cependant, ce cadre de référence socio-technique mis à l'épreuve n'acquiert pas pour autant la forme de stabilisation la plus robuste qui soit. Comme annoncé en début de partie, le processus de stabilisation n'est pas achevé et il serait erroné, en absence d'usages effectifs, de conclure en la concrétisation d'un alliage/boîte noire pour l'ensemble des acteurs potentiellement concernés par l'usage du dispositif. En effectuant ce test, c'est un premier indice de la

---

<sup>155</sup> Pour plus de détails sur la méthodologie CAUTIC, se reporter au chapitre II de la partie I.

capacité de l'invention à se muer en innovation qui était recherché. Plus spécifiquement, c'est la capacité de la projection d'usage à voyager hors des terres de l'équipe-projet qui était éprouvée.

Figure 13. Tableau croisé des réponses données par chaque interviewé pour chaque critère évalué. Extrait du rapport produit par l'Uman Lab : « User & Social Acceptance »

	Criteria															
	Know-how				Practice				Identity				Social environment			
	1.1	1.2	1.3	1.4	2.1	2.2	2.3	2.4	3.1	3.2	3.3	3.4	4.1	4.2	4.3	4.4
Interviews																
#01																
#02																
#03																
#04																
#05																
#06																
#07 Bank																
#08																
#09																
#10 Transport																

Enfin, le déroulement du projet témoigne de l'importance prise au fil du temps par les scénarios et de la confiance émise par l'équipe-projet dans la capacité à cette objet intermédiaire de conception à synthétiser. Le scénario, matérialisation ad hoc de la projection d'usage, est donc un objet intermédiaire de conception structurant de Fuzzy Front End de l'innovation. Nous allons maintenant nous pencher plus précisément sur les modalités

## VI - La scénarisation comme modalité de projection

---

La suite de notre étude empirique se limitera à la première phase du projet (WP1), intitulé « Privacy for contactless and threats analysis », et sera dédiée à l'étude de la tâche 1.1 soit l'élaboration des scénarios d'usage du concept du CPM, Contactless Privacy Manager. L'écriture de ces scénarios devra prendre appui sur deux livrables : un état de l'art de la technologie sans contact et des problèmes qu'elle pose en rapport avec la notion de « Privacy » et un état de l'art dédié aux solutions de protections déjà existantes. Les scénarios serviront de base à l'élaboration de spécifications fonctionnelles d'un dispositif de protection idéal précédant la sélection de l'éventail des fonctionnalités à intégrer dans le démonstrateur.

L'attention que nous portons au travail de scénarisation tient de ce qu'il fait partie de l'activité sociotechnique que constitue le processus de conception (Bucciarelli, 1994 ; Vinck, 1999). Il vise à la production d'un objet, le scénario, dont l'usage correspond à des réalités différentes selon les domaines d'utilisation dans le champ de la conception technologique. Ainsi, la notion de « scenario-based design », la conception fondée sur les scénarios, recouvre des pratiques hétéroclites. Cette hétérogénéité alimente l'équivocité de la notion de scénario. Dans les lignes qui suivent, nous désirons saisir les réalités multiples que recouvre le terme afin de pouvoir mieux situer l'objet dont la construction va servir de base à notre analyse.

Dans les champs du développement de systèmes informatiques et du génie logiciel, les « cas d'utilisation » (use cases) ont un emploi éprouvé :

*« Un cas d'utilisation établit, entre les différents intervenants, un contrat régissant le comportement d'un système. Il décrit ce comportement sous diverses conditions, lorsque le système répond à une requête émanant de l'un des intervenants, appelé acteur principal. L'acteur principal amorce une interaction avec le système en vue d'atteindre un objectif particulier. Le système répond, en veillant à protéger les intérêts de tous les intervenants. Diverses séquences de comportement, ou scénarios, peuvent se déployer, en fonction des requêtes effectuées et des conditions de leur réalisation. Le cas d'utilisation regroupe ces différents scénarios. »* (Cockburn, 2001 p. 1)



Ce sont donc des descriptions abstraites qui anticipent les actions de l'utilisateur face à un logiciel ou un système informatique et visent à améliorer l'utilisabilité<sup>156</sup> des dispositifs technologiques (Jacobson, 1995). Cet objectif est parfois désigné comme celui de « *usability engineering* » - l'ingénierie de l'utilisabilité, « *a process whereby the usability of a product is specified quantitatively, and in advance* » (Tyldesley, 1988). Champ voisin du l'ingénierie de l'utilisabilité, le « *requirement engineering*<sup>157</sup> » - l'ingénierie des besoins, utilise le processus de « *requirement elicitation* » - la formalisation des besoins, pour comprendre les spécificités du domaine d'application, le problème à être résolu, les besoins et contraintes organisationnels, et les besoins des acteurs du système développé (Kujala, 2002). Ici, l'usage du scénario est généralisé mais l'utilisateur n'est pas considéré comme un acteur plus important que d'autres du dispositif en développement.

Cependant, cette recherche de perfectionnement de l'utilisabilité des artefacts par le recours aux « *cas d'utilisation* » s'est enrichie au contact de chercheurs désireux de réactualiser la place de l'usager dans le processus de conception. Cette tendance, nommée conception centrée-utilisateur (User-Centred Design - UCD<sup>158</sup>) va occasionner des recherches approfondies sur les méthodologies d'appui à la conception. C'est dans le champ des « *interactions homme-machine* » (Human-Computer Interaction - HCI<sup>159</sup>) d'une part, et de la « *conception participative* » (Participatory Design - PD<sup>160</sup>) d'autre part, que les

<sup>156</sup> L'utilisabilité est définie par la norme ISO 9241 comme « le degré selon lequel un produit peut être utilisé, par des utilisateurs identifiés, pour atteindre des buts définis avec efficacité, efficience et satisfaction, dans un contexte d'utilisation spécifié. »

<sup>157</sup> « [Requirement engineering] is a subdiscipline of systems engineering and software engineering that is concerned with determining the goals, functions, and constraints of hardware and software systems. » (Laplante, 2007 p. 44). Marc Berg, dans un article critique sur la conception technologique souligne l'aspect dépassé de ces philosophies de conception : « Traditional systems design » is the starting (and counter) point of most stories. Design here starts with system requirements: a list of functional demands the information technology (IT) should meet. The list should be detailed, exhaustive, and clear-cut, so that computer scientists can focus fully on their real task of designing an efficient system that fulfills these requirements efficiently, smoothly, and aesthetically. This usually implies making a model of the work practice that the system should function in: the flow of work, the sequencing of tasks, the hierarchy of responsibility and control, and so forth. The acquisition of the requirements is seen to be a preliminary step, a prerequisite for the real work to start. It consists primarily of asking those who have ordered the system what exactly they want the system to do. Those who order new information technologies, however, are often not the same people who work with the technologies, and often those who put together the requirements are not the same people who do the actual design. » (Berg, 1998 p. 461)

<sup>158</sup> Cette forme de conception est ainsi définie par Karat : « The goal of user-centered design is the development of useful and usable products, although there appears to be no agreed-on definition or process for it. » (Karat, 1997 p. 36-37) Elle repose sur trois principes énoncés dans un article princeps (Gould & Lewis, 1985) : une attention anticipée tournée vers l'usager et les tâches qu'il doit accomplir, l'équipement en instruments de mesure empiriques, l'itérativité du processus de conception. Ces principes fondateurs ont ouvert la voie à de nombreux développements qui ont, sur le plan opérationnel, débouchés en 1999 sur l'élaboration de la norme internationale ISO 13407 qui définit les activités caractéristiques du UCD et fournit des indications pour suivre ce process.

<sup>159</sup> « Human-computer interaction (or HCI) is, put simply, the study of people, computer technology and the ways these influence each other. We study HCI to determine how we can make this computer technology more usable by people. This requires an understanding of at least three things: the computer technology, the people who interact with it and what is meant by more usable. However, there is a fourth aspect which is implicit in the simple definition: understanding the work that people are trying to perform by using the technology. » (Dix, Finlay, Abowd & Beale, 1993 p. xiii). Au départ concentré autour des sciences cognitives, le champ de HCI s'est considérablement ouvert à d'autres univers aujourd'hui : cognition distribuée, théorie de l'activité, ethnométhodologie.

<sup>160</sup> Approche de la conception d'inspiration syndicale développée dans les pays scandinaves dans les années 70. L'objectif est de rétablir un équilibre entre usagers des technologies et politiques volontaristes des concepteurs en associant les

réflexions ont été les plus foisonnantes. Ces travaux ont notamment débouché sur une diversification des usages des scénarios dans la conception technologique.

En HCI, l'utilisateur n'est plus considéré du point de vue restreint de la rencontre entre un utilisateur et un artefact : la question posée est celle de l'intégration de l'artefact dans un environnement professionnel puis, plus tard, de l'intégration des artefacts dans d'autres environnements (Preece, Rogers & Sharp, 2002 ; Bell, Genevieve *et al.*, 2003 ; Blythe, Wright, McCarthy & W. Bertelsen, 2006 ; Sengers & Gaver, 2006). La diffusion de l'électronique et de l'informatique dans d'autres objets que l'ordinateur a favorisé l'élargissement du champ de compréhension de l'utilisateur. Cet élargissement des objets du HCI s'inscrit dans un mouvement plus large, inspiré par la philosophie pragmatique, et focalisé sur « *l'expérience*<sup>161</sup> » de l'utilisateur. Ainsi, chercheurs et praticiens ont dépassé la compréhension stricte de l'utilisabilité pour embrasser des thématiques telles que l'amusement (Blythe, Overbeeke, Monk & Wright, 2003), la beauté (Cooper, A., 1999 ; Hassenzahl, 2004), les valeurs (Petersen, Luvigsen, Jensen & Thomsen, 2004) ou encore les émotions (Norman, 2004). Sur le plan organisationnel, l'utilisabilité cesse de n'être envisagée que comme une étape donnée du processus de conception ; elle est une donnée constante à maximiser (Carroll, John, M. , 1996), notamment par le recours aux scénarios<sup>162</sup> :

*« The role of usability changes from being an activity that approves of a computer application, to an activity that takes responsibility for the product and its future use, by being part of the design process. »* (Bodker, 1999 p. 62)

Dans le même sens, se développe un mouvement critique de dépassement de l'utilisabilité comme objectif ultime, mouvement qui octroie à l'utilisateur une compétence à participer à l'activité de conception. Plus qu'un usager virtuel face à une interface informatique, l'utilisateur devient contributeur actif d'un processus de conception itératif

---

usagers à la conception technologique. Pour plus de renseignements, on peut lire : (Grudin, 1993 ; Bjerknes & Bratteteig, 1995 ; Kensing & Blomberg, 1998 ; Sanders, 2002)

<sup>161</sup> Dans le champ de la conception, l'expérience ne bénéficie pas d'une définition univoque. Cependant, l'accent est mis sur la subjectivité de l'expérience vécue ou à vivre ainsi que sur la définition du contexte d'usage comme finalité du design (Battarbee, 2003). Voir également la première partie de la thèse et la pratique sibylline de l'usage.

<sup>162</sup> « Scenarios of human-computer interaction help us to understand and to create computer systems and applications as artifacts of human activity – as things to learn from, as tools to use in one's work, as media for interacting with other people. Scenario-based design of information technology addresses five technical challenges: Scenarios evoke reflection in the content of design work, helping developers coordinate design action and reflection. Scenarios are at once concrete and flexible, helping developers manage the fluidity of design situations. Scenarios afford multiple views of an interaction, diverse kinds and amounts of detailing, helping developers manage the many consequences entailed by any given design move. Scenarios can also be abstracted and categorized, helping designers to recognize, capture and reuse generalizations, and to address the challenge that technical knowledge often lags the needs of technical design. Finally, scenarios promote work-oriented communication among stakeholders, helping to make design activities more accessible to the great variety of expertise that can contribute to design, and dressing the challenge that external constraints designers and clients often distract attention from the needs and concerns of the people who will use the technology. » (Carroll, 1999)

(Bodker, 1996 ; Preece, Rogers & Sharp, 2002). La question des moyens d'implication de l'utilisateur se trouve au cœur des recherches en conception participative. C'est dans ce cadre que le scénario a été interrogé tant d'un point de vue formel que sur la question des objectifs poursuivis. Les thèmes abordés concernent ainsi l'utilisation de schémas de narration (Clausen, 1993), d'histoires contées (Erickson, 1995), l'importance des scénarios dans la prise de décision (Norman, 1993), la différence d'impact sur l'attitude entre descriptions techniques et scénarios (Storm, 2003), l'opportunité d'usage du support vidéo (Tognazzini, 1994) ou encore la question de l'épaisseur de description des personnages présents dans le scénario (Cooper, A., 1999 ; Nielsen, 2002 ; 2004).

Bien qu'il existe aujourd'hui un consensus transdisciplinaire sur l'effectivité des rôles du scénario hors du domaine de l'utilisabilité (Navarro, Forest, Lavoisy & Chanal, 2009), demeure toujours une ligne de démarcation subtile au niveau téléologique et qui trouve son expression sur le plan formel. Selon qu'ils soient orientés vers l'accomplissement de tâches<sup>163</sup> (« *task-driven scenarios* ») ou vers des histoires centrées sur « l'humain<sup>164</sup> » (« *human-centered stories* »), les scénarios partagent alors la même dénomination mais renvoient à des réalités éloignées, reflet d'objectifs de recherche et de conception différents. Cette opposition permet également de comprendre la variété des objectifs poursuivis lors du recours aux scénarios :

« *Scenarios, thus, are constructions made with a purpose. This purpose helps scenario constructors to be selective. The purpose may relate to both the type of situation the scenario is dealing with and to the type of design situation that the constructors want to support.* » (Bodker, 1999)

Susan Bodker, en se basant sur la nomenclature établie par Kyng (1995), distingue ainsi trois types d'objectifs poursuivis lors de l'utilisation de scénarios : présenter des solutions dans un contexte, illustrer des solutions alternatives et identifier des problèmes potentiels. L'auteure souligne, par ailleurs, la nécessité d'adapter la forme et le contenu de la description en fonction de l'étape de conception durant laquelle le scénario est mobilisé. Selon celle-ci, les scénarios devront présenter des situations typiques ou critiques (Carroll, John, M. , 1996), exposer les situations de manière plus ou moins ouverte ou encore opter ou non pour des descriptions caricaturales.

<sup>163</sup> « [...] the plots, the progression of events in the scenarios, are made to illustrate a specific task or the use of a specific artifact. » (Storm, 2003 p. 912)

<sup>164</sup> « Similar to published fiction short stories [...] characterized by being driven by the motivations and emotions of the characters in it, and by having built in obstacles or conflicts that the characters try to overcome. Human-centered stories are further characterized by the use of dialogue or directly quoted speech, to show the personalities and emotions of the characters and to heighten the feeling of conflict. » (Storm, 2003 p. 912)

Par ailleurs, l'antagonisme entre les scénarios orientés vers l'accomplissement de tâches et ceux construits sur des histoires centrées sur « l'humain » s'inscrit dans la logique qui oppose les scénarios comme outil d'évaluation aux scénarios comme moyen d'exploration (Sengers & Gaver, 2006), comme « *tremplins*<sup>165</sup> » (Bodker & Christiansen, 1997). Cette notion de tremplin illustre l'enthousiasme des auteures pour l'utilisation des scénarios dans le contexte de la conception, contexte qu'elles considèrent comme un champ de tensions entre l'action et la réflexion :

*« Design is a particular kind of activity that crosses, or lives on, the boundaries of several communities of practice relating the future to the past. Design processes have a double orientation: toward the product and toward the process. Because what is going to be created is by definition new and unknown, at least to some extent, neither product nor process can be fully known or planned in advance. »* (Bodker & Christiansen, 1997 p. 221)

Cette réflexion sur les utilisations variées des scénarios durant les projets de conception participe d'un mouvement plus large de remise en question de la linéarité et de la rigidité du processus de conception et de réflexion sur les représentations tangibles mobilisées durant l'activité de conception (Floyd, 1987 ; Griesemer & Star, 1989 ; Greenbaum & Kyng, 1991 ; Henderson, 1991 ; Carroll, John, M. , 1996 ; Vinck & Laureillard, 1996 ; Bodker, 1998 ; Henderson, 1998 ; Jeantet, 1998 ; Highsmith, 2002). Les travaux réflexifs portant sur l'objet scénario s'inscrivent ainsi dans ce mouvement qui s'intéresse aux prototypes, schémas, cartes, maquettes, et autres dessins mobilisés durant la conception.

Cette appréhension de la conception comme un champ de tensions est à mettre en relation avec le centre d'intérêt de notre étude et le choix de la scénarisation comme entrée. En tant que support et moyen mobilisé durant la conception, le scénario fait partie de la galaxie des objets intermédiaires de la conception (OIC)<sup>166</sup>. En cela, l'analyse de sa construction et sa circulation durant la conception permet de mettre à jour les dynamiques du processus de conception :

<sup>165</sup> Le concept est emprunté au cognitiviste Engeström : « A springboard is a facilitative image, technique or socio-conversational constellation... misplaced or transplanted from some previous context into a new. » (p. 287). « Springboards do not come about smoothly or automatically, and they are not as such solutions to the problem that one is facing. They are starters that may lead to an expansive solution. » (Bodker & Christiansen, 1997 p. 220)

<sup>166</sup> « Il s'agit des objets produits ou utilisés au cours du processus de conception, traces et supports de l'action de concevoir, en relation avec outils, procédures, et acteurs. Son contenu empirique peut rester flou et n'être déterminé qu'au cas par cas selon ce qui se présente sur chaque terrain. Son intérêt est de nous permettre de disposer d'une notion de même niveau de généralité que celle d'« organisation » pour poser les questions relatives à l'étude des processus rencontrés sans faire abstraction de leur contenu, de leur instrumentation et de leur manière concrète de fonctionner. » (Jeantet, 1998 p. 293-294)

*« Si nous nous intéressons aux objets intermédiaires de la conception, ce n'est pas par je ne sais quelle curiosité d'entomologiste, ou quel parti pris positiviste ou fétichiste, mais parce que, de fait, tout au long du processus de conception ils sont produits, circulent, orientent, contraignent, ou sont mis à l'épreuve, critiqués, corrigés, complétés, bref constituent au minimum un support, quand ce n'est pas un partenaire, au travail des acteurs engagés dans le processus. En les suivant à la trace, on peut donc à la fois reconstituer le réseau de concepteurs effectivement à l'œuvre (et pas seulement celui qu'indique l'organigramme ou le planning), en même temps que l'on suit l'avancée de la conception, qu'on en décèle les modalités de fonctionnement, les moments d'ouverture, de négociation, ou au contraire de clôture, de décision et de création d'irréversibilités, et les points sur lesquels portent ces moments. Bref, les objets intermédiaires sont d'abord pour nous des analyseurs qui permettent d'accéder à la réalité des processus effectifs de conception. » (Jeantet, 1998 p. 296)*

Les trois registres conceptuels par lesquels appréhender les OIC n'ont pas perdu en pertinence ; on les retrouve même sous des formes proches au sein de travaux qui tirent des conclusions similaires (Vinck, 1995 ; Bodker & Christiansen, 1997 ; Henderson, 1998 ; Bodker, 1999 ; Bowker & Star, 1999 ; Carlile, 2002 ; Boujut & Blanco, 2003 ; Carroll, John, Rosson & McInerney, 2003 ; Lee, 2007)<sup>167</sup>. Ils permettent d'appréhender les rôles joués par ces artefacts durant le processus de conception en décortiquant leur triple apport par leurs qualités de médiation, de traduction et de représentation (Vinck & Laureillard, 1996 ; Jeantet, 1998 ; Boujut & Blanco, 2003).

Cependant, comprendre les scénarios comme OIC ne suffit pas pleinement à les appréhender dans le contexte de notre étude. Le concept est, en effet, doté d'une puissance heuristique peu commode pour notre entreprise. D'abord, parce que le concept d'OIC aborde l'activité de conception d'un point de vue longitudinal, de l'émergence d'une idée à sa réalisation matérielle. Presque à l'opposé, notre focale empirique se restreint à une séquence précise du processus de conception : le lieu d'élaboration de la projection d'usage. Ainsi, il ne s'agit pas de prendre en compte l'intégralité du processus de conception dans notre champ d'analyse mais de centrer notre attention sur l'une de ces étapes. Aussi, nous avons témoigné du fait que le scénario, dans le champ de la conception, recouvre des usages différents voire antagonistes et que chacun de ces usages sont eux-mêmes traversés de

<sup>167</sup> Pour un compte-rendu bibliographique exhaustif, on se reportera à (Trompette & Vinck, 2009)

tensions quant aux objectifs à poursuivre. Ainsi, nous souhaitons nous concentrer sur la structuration de ces champs de tensions dans notre travail empirique. De ce fait, il nous faut évacuer la qualité « intermédiaire » de ces objets et leur préférer une démarche analytique écologique à une démarche proche de l'esprit de celle de l'acteur-réseau<sup>168</sup> (Fujimura, 1992). Il s'agit ainsi de mettre l'accent sur les formes effectives de coordination entre acteurs et objets, de comprendre la mécanique des processus d'alignement entre coopération et hétérogénéité et de rendre compte du « *poids des inerties dont se chargent les infrastructures de communications* » (Trompette & Vinck, 2009 p. 3), dans le cadre d'une collaboration entre sciences sociales et sciences pour l'ingénieur. Pour ce faire, nous nous armons de deux outils encadrant pour notre travail d'analyse, deux outils qui maintiennent une filiation certaine avec le concept d'OIC.

Il s'agit d'abord d'adopter une définition des scénarios suffisamment large pour ne pas préempter l'analyse mais suffisamment précise pour situer ceux-ci dans le champ de la conception. Ainsi, nous reprenons la définition proposée par Annie Gentès. Pour elle, ces types d'objet « *décrivent ce que la technique devra faire (ils ont ainsi une valeur contractuelle) et donnent les pistes pour la fabrication, à la fin d'un projet, d'un démonstrateur – qui devra comme son nom l'indique, démontrer que l'objet technique fonctionne et qu'il rend un service.* » (Gentès, 2008 p. 84)

Par ailleurs, comprendre les scénarios comme des OIC forme une première étape d'analyse nécessaire mais insuffisante à appréhender ceux-ci comme outil stratégique d'une étape de conception particulière. Dès lors, c'est la volonté de ne pas rapatrier brutalement ces outils conceptuels au risque de les tordre qui a stimulé notre recherche d'outils connectés mais plus adaptés aux particularités de notre terrain. C'est au sein de la galaxie des sociologies réhabilitant la prise en compte des objets que nous avons trouvé un concept adapté à notre investigation : le concept d'« *objet-frontière* » (Bowker & Star, 1999). Ce concept, qui décrit ces objets facteurs de succès dans la coopération entre différentes communautés de pratique, est ainsi défini :

*« Boundary objects are those objects that both inhabit several communities of practice and satisfy the informational requirements of each of them. Boundary objects are*

<sup>168</sup> Bien que le concept d'OIC n'appartienne pas explicitement au vocabulaire associé à la théorie de l'acteur-réseau, nous considérons qu'il s'inscrit dans une démarche de réhabilitation du traitement des objets dans l'analyse des activités sociales. En ce sens, le concept d'OIC participe d'un mouvement sociologique plus large que la théorie de l'acteur-réseau mais dont celle-ci constitue l'étendard le plus médiatique.

*thus both plastic enough to adapt to local needs and constraints of the several parties employing them, yet robust enough to maintain a common identity across sites. They are weakly structured in common use and become strongly structured in individual-site use. These objects may be abstract or concrete. [...]Such objects have different meanings in different social worlds but their structure is common enough to more than one world to make them recognizable, a means of translation. The creation and management of boundary objects is a key process in developing and maintaining coherence across intersecting communities. » (Bowker & Star, 1999 p. 297)*

C'est donc sur ce concept et sur les réflexions inspirées par celui-ci que nous nous appuierons pour mener notre réflexion. Celle-ci sera orientée sur l'hypothèse de départ que les scénarios constituent des « objets-frontières. »

## VII - L'observation participante comme méthode d'investigation

---

Le choix de l'observation s'explique par la volonté de suivre au plus près le développement méthodologique que constitue le travail de scénarisation de l'usage sans porter atteinte au déroulement de celui-ci :

*« L'observation consiste à se trouver présent et mêlé à une situation sociale pour l'enregistrer et l'interpréter en s'efforçant de ne pas la modifier. Cette situation sociale est toujours le produit d'une interaction entre les participants eux-mêmes et, d'une façon ou d'une autre, entre les participants et l'observateur ; elle prend la forme d'évènements composés de séquences successives avec un début et une fin. »* (Peretz, 2004 p. 5)

Ainsi, la volonté de verser à l'observation une couche de participation est moins motivée par une volonté de modification ou d'expérimentation au sens scientifique du terme, que par la nécessité de toucher du doigt les faits et à se familiariser rapidement au contexte de travail, fut-il ancré hors de l'usine :

*« On appelle observation participante en usine le fait, pour un sociologue, de participer, en tant que salarié, à la production dans l'entreprise pour en tirer l'information et la documentation la plus proche des faits et du travail concret. Cette participation se déroule généralement sur une longue période (trois mois à un an (...)) de manière à s'intégrer dans le collectif de travail, à se familiariser avec la forme spécifique de l'activité et à contrôler sur un grand nombre de cas les analyses dégagées. »* (Peneff, 1996)

Cette méthode d'investigation nous paraissait ainsi la plus adaptée à suivre à la fois la construction des scénarios et l'action de ses producteurs tout en tenant compte des contraintes empiriques qui sont les nôtres. Elle posait cependant des questions importantes concernant notre engagement dans cette activité.

### ***A - L'OP comme moyen de suivre les acteurs/actants.***

L'adoption de l'observation participante comme méthode d'investigation participe de deux éléments. Ce choix est, d'une part motivé, par nos objectifs de recherche, d'autre part, contraint par les conditions matérielles d'accès au matériau empirique.



En participant à un projet de conception innovante dès sa genèse nous souhaitons considérer la projection d'usage telle qu'elle se fait<sup>169</sup>. Cette posture de recherche, faite injonction par les tenants des approches constructivistes de l'innovation, opère comme un garde-fou méthodologique à la tentation déterministe. Relevant le lien latent entre compréhension essentialiste de la technologie et déterminisme technologique, Madeleine Akrich affirme ainsi :

*« Indeed, because it ignores the wide range of uses to which objects may be put, it comes close to technological determinism. It is obvious that it cannot possibly explain the wide variety of fates experienced by technological projects—fates that range from complete success to total failure. One way of approaching the problem is to follow the negotiations between the innovator and potential users and to study the way in which the results of such negotiations are translated into technological form. Indeed, this method has been widely used in sociological and historical studies of technology. Thus, if we are interested in technical objects and not in chimera, we cannot be satisfied methodologically with the designer's or user's point of view alone. Instead we have to go back and forth continually between the designer and the user, between the designer's projected user and the real user, between the world inscribed in the object and the world described by its displacement. »* (Akrich, 1992 p. 208-209)

Deux enseignements principaux sont à tirer de cet extrait au regard de nos objectifs de recherche. Retenons d'abord ce qu'il contient de congruent avec notre étude. L'accent mis sur le déplacement (« *displacement* ») de l'objet comme révélateur de *mondes* décrits ou inscrits par/en lui s'accorde avec notre volonté de *poursuivre* le processus de création de l'usage projeté comme moyen d'accès à la trajectoire de cet objet, de ces reconfigurations d'une main à l'autre, de mondes à mondes. En d'autres termes, s'intéresser au déplacement de l'objet c'est s'intéresser à la politique comme processus d'ordonnancement de collectifs.

Cependant, le lecteur a sans doute perçu l'opportunisme bancal de l'emploi d'une telle référence dans notre cas d'espèce. Tandis que Madeleine Akrich insiste sur les allers-retours entre utilisateurs réels et concepteurs comme ponctuations indispensables à l'analyse de la destinée (« *fate* ») d'un objet, notre étude semble se contraindre à l'analyse de ce qu'elle nomme astucieusement des « *chimères* », soit une analyse restreinte au point de vue des concepteurs. Or, l'opposabilité d'un tel argument est mise en jeu dès lors qu'il est admis que notre entreprise ne vise pas à l'élucidation du destin d'un produit final. En plaçant la focale sur le versant méthodologique des processus d'innovation, nous procédons, de manière quasi

---

<sup>169</sup> Nous pastichons ici la formule de (Latour, 1987 ; Latour & Callon, 1991)

mécanique, au décentrage de l'intérêt analytique vers les OIC. Par cette opération, nous transfigurons le concepteur<sup>170</sup> en lui reconnaissant plus que la qualité de construire l'utilisateur à partir de lui-même comme premier utilisateur de l'objet (Woolgar, 1991 ; Carlson, 1992 ; Bardini & Horvath, 1995) : le concepteur est ici utilisateur exclusif de l'objet en conception, qu'il s'agisse largement du concept ou de manière plus étroite du scénario.

Ceci dit, question reste posée de l'espace empirique à l'intérieur duquel nous désirons évoluer. Le succès rencontré par les analyses constructivistes du développement technologique ne pourrait être compris sans considérer le privilège dont jouissent les chercheurs dans la constitution de leur terrain de recherche. L'« *hindsight* »<sup>171</sup>, c'est-à-dire le bénéfice de l'analyse rétrospective, procuré par une approche socio-historique de l'innovation réduit sensiblement les contraintes spatio-temporelles qui compriment le volume d'action du chercheur : l'examen des processus de stabilisation et de fermeture des controverses liées au dispositif technique ainsi que le travail d'identification des groupes sociaux pertinents peuvent s'effectuer dans une quiétude minutieuse. Prenons par exemple l'étude princeps de Pinch et Bijker sur le développement de la bicyclette<sup>172</sup>. L'identification et l'étude des groupes sociaux pertinentes, « *relevant social groups* », se manifestent par l'intermédiaire de documents produits en des lieux et endroits différents mais rendus simultanément disponibles à l'analyse par le jeu d'une mise à plat du temps et de l'espace. Cependant, parce que ces documents révèlent des trajectoires, des négociations, soit que l'analyste par leurs confrontations fasse lumière sur ces débats, soit que ceux-ci témoignent de ces disputes, leur accès permet de suivre des acteurs dont l'inactivité est de fait une caractéristique contemporaine de l'activité de recherche. Par ailleurs, tandis que la méthode ethnographique rencontre les faveurs de la plupart des chercheurs constructivistes<sup>173</sup>, ce sont

<sup>170</sup> L'emploi du mot *concepteur*, ainsi que de celui d'*utilisateur*, au singulier doit être comprise non pas comme une réduction de la diversité des manières d'être de l'un ou l'autre, mais plutôt au regard d'une distribution des prérogatives régulièrement convoquées dans le jeu de la conception. Leur emploi fait ainsi écho lointain à celui qui est fait du terme législateur, dans le domaine politique, celui-ci désignant l'assemblée investie du pouvoir de légiférer. Ainsi, le concepteur l'est de celui de concevoir, l'utilisateur de celui d'utiliser.

<sup>171</sup> Nous traduisons ce terme par sagesse rétrospective. « For we are able to say that technical objects changed, stabilized, naturalized, or depoliticized social relations only with the benefit of hindsight. It is only after the event that causes are stabilized. And it is only after the event that we are able to say that objects do this, while human beings do that. It is in this sense, and only in this sense, that technical objects build our history for us and «impose» certain frameworks. And it is only for this reason that an anthropology of technology is both possible and necessary. » (Akrich, 1992 p. 222). Notre idée fait également écho à ce que Pierre Bourdieu appelle le privilège de la totalisation : « la capacité de se donner et de donner la vue synoptique de la totalité et de l'unité des relations qui est la condition du déchiffrement adéquat. » (Bourdieu, 1980 p. 138-139)

<sup>172</sup> On comprend alors pourquoi Bijker se réjouit de la facilité à suivre les acteurs : « It is relatively easy to identify the relevant social groups by « following the actors ». They are themselves quite explicit about it. » (Bijker, 1992 p. 76)

<sup>173</sup> Voir l'étude plaidoyer de Bruno Latour et Steve Woolgar dans laquelle la fabrique des faits scientifiques est rendue accessible par l'observation anthropologique du travail quotidien des employés de laboratoires, celui-ci étant devant être appréhendé comme un objet doté d'*étrangeté anthropologique* pour les sociologues l'étudiant (1979). Notons que Bijker célèbre également les qualités préventives de ce type d'approche : « Actors provide an effective starting point from which

cette fois-ci les formes mêmes de notre terrain qui nous y empêchent d'y avoir recours complètement. L'éloignement géographique des partenaires, tout autant que l'organisation même du projet<sup>174</sup>, expliquent principalement l'impossibilité pour un *non-ubiquiste* de suivre l'ensemble de ceux que nous définissons comme *nos groupes sociaux pertinents*, soit les membres du projet. Le choix de l'observation participante procède ainsi d'un arbitrage contraint fondé sur la présomption que la présence aux lieux de prise de décision collective pouvait nous ouvrir l'accès aux traces et indices d'un *réel* exposé lors de ces moments dédiés à la négociation. Ainsi, loin de constituer un grossier succédané méthodologique, le choix de l'observation participante traduit une prise en compte de contraintes analytiques et matérielles. Il est adaptation de l'instrumentation à l'investigation comme le préconise Howard Becker dans cet extrait :

*« Nous ne devons pas décider que seul le travail de terrain peut fournir des preuves dignes de foi pour arriver à des conclusions sociologiques. De nombreuses personnes ont montré incontestablement que nous devrions employer des méthodes appropriées à la forme de notre problème et aux caractéristiques du monde que nous étudions. Là où le travail de terrain est la méthode appropriée, néanmoins, le point fort de mon argument est que nous pouvons employer les indices qu'il produit sans s'inquiéter inutilement. Puisqu'ils nous fournissent des informations sur des gens qui agissent sous les contraintes sociales mêmes auxquelles nous nous intéressons, et parce que les nombreuses informations et les procédures flexibles nous permettent de tester nos conclusions de façon répétée et de diverses manières, nous ne devons pas craindre que leur caractère peu systématique déforme nos résultats de la façon que nous, nos lecteurs ou les personnes que nous étudions, trouvons commode, convenable, ou à laquelle nous nous attendons. »* (Becker, 2006 p. 97)

Par ailleurs, la construction de notre matériau empirique ouvre la voie à une qualification théorique de notre espace d'observation et d'analyse comme « *réseau local* ». La distinction apportée par Michel Callon et John Law entre réseaux globaux et réseaux

---

to identify relevant social groups. In that sense, « relevant social group » is an actor category. However, it is indeed only a starting point, and this method is not proposed as an « idiot-proof » recipe for carrying out a social constructivist case study. For example, it may be difficult to decide whom to treat as spokespersons for a specific relevant social group, although this will, again, often become clear if we let the actors speak for themselves. In some instances—for example, when one social group is splitting in two—groups may not accept someone acting as its spokesperson, but that will again become evident by « listening » to the actors. Another problem is that only « vocal » attributions of meaning are analyzed, and there is always the danger of the analyst not « hearing » the voices of some parties. This ethnographic approach deliberately focuses on meanings attributed to artifacts and does not take the route of imputing hidden interests to social groups as, for example, Marxist structuralism or Parsonian functionalism would do. » (Bijker, 1992 p. 77)

<sup>174</sup> De fait, cet éloignement géographique ne permet pas la prise en compte de la littérature abondante en HCI ou CSCW concernant les processus de conception en groupes restreints (« *small group design process* ») notamment caractérisés par le partage d'un espace, de ressources physiques et d'action conjointe. (Tang, 1991 ; Lloyd, 2000 ; Dourish, 2001). Nous portons également une attention toute limitée aux formes de collaboration engagées dans les processus de communication à l'intérieur ou à l'extérieur de l'équipe-projet.

locaux dans leur étude de la conception de l'avion TSR.2. (Callon & Law, 1989), démontrait que le succès de la conception reposait notamment sur l'existence d'intermédiaires entre ces réseaux. Elle nous est ici néanmoins utile à caractériser le projet COPRIM comme un processus d'élaboration d'un réseau local au sein d'un espace de négociation (« *negociation space* ») déterminé :

*« We have considered the way in which an actor attempts to mobilize and stabilize what we call a global network in order to obtain resources with which to build a project. In our language, then, a global network is a set of relations between an actor and its neighbors on the one hand, and between those neighbors on the other. It is a network that is built up, deliberately or otherwise, and that generates a space, a period of time, and a set of resources in which innovation may take place. Within this space—we call it a negotiation space—the process of building a project may be treated as the elaboration of a local network—that is, the development of an array of the heterogeneous set of bits and pieces that is necessary to the successful production of any working device. »* (Law & Callon, 1992 p. 21-22)

La caractérisation du projet comme réseau local permet d'appréhender le dimensionnement et la structuration de l'espace de négociation au sein duquel va prendre place l'observation participante. Rappelons-le, le projet COPRIM (COnтактless Privacy Manager) est un projet de recherche industrielle multipartenaires d'une durée de trois ans (2007-2010) bénéficiant du soutien de l'ANR. Ainsi, tandis que le projet respecte l'ensemble des critères ayant présidé à la sélection de nos terrains empiriques<sup>175</sup>, l'examen de son amorce permet d'évoquer le réseau global dont il est partie à travers le contexte particulier d'association des sciences sociales à cette initiative de conception. Dans notre cas d'espèce, tandis que le montage du projet s'est déroulé sans que les technologues ne considèrent *a priori* l'utilité d'y associer des SHS, l'ANR a considéré cette association nécessaire au vu de la nature du projet. Rédigée en anglais<sup>176</sup>, l'annexe technique<sup>177</sup> au projet fait place honorable au concept de « Privacy » difficilement traduisible en français comme l'indique Bénédicte Sirey :

*« Littéralement, le terme de « Privacy » peut se traduire par le fait d'être seul, par l'expression « vie privée », ainsi que par les termes de secret, et d'intimité. Le terme anglais de « Privacy » n'a donc pas de transcription unique en français, même si l'expression de*

---

<sup>175</sup> Cf. introduction.

<sup>176</sup> L'anglais constitue, en sciences dures, la *lingua franca* et *scientifica* par excellence, même entre partenaires francophones.

<sup>177</sup> Voir annexe 4.

« vie privée » lui vaut traduction dans nombre de textes. Dans le cas plus précis des sites Internet, les sites anglo-saxons affichent une rubrique « Privacy Policy ». Les sites français proposent alternativement une rubrique intitulée « politique de confidentialité », ou « protection des données personnelles. » (Sirey, 2007 p. 2)

On peut raisonnablement penser que l'opération de traduction du terme de l'anglais au français ait eu un poids important dans la nécessité reconnue d'associer des SHS au projet COPRIM. Tandis que les projets technologiques se saisissent du terme comme synthétisant l'ensemble des questionnements techniques liés à la protection des données personnelles, la « Privacy » peut faire l'objet d'une acception où le social l'emporte, celle de la vie privée. L'extrait d'interview du chef de projet semble valider notre interprétation :

*« Comme il s'agissait de protection de la vie privée, l'ANR nous, enfin, a labellisé le projet mais nous a suggéré de faire rentrer un partenaire des sciences humaines et sociales. Donc on est allé voir X, qui était à côté, spécialisé dans ce domaine-là, pour être dans le projet. Et donc, X amène la composante à la fois analyse des ressentis, des besoins des utilisateurs par rapport à la technologie sans contact, et en particulier le NFC dans ce projet-là. Et après, alors, ça, c'est dans une première phase d'étude des scénarios. »* (Entretiens SHS/Innovation : Interview du chef de projet COPRIM<sup>178</sup>)

Ainsi, l'ANR, en identifiant implicitement la « Privacy » à la vie privée, a procédé à un profond remaniement de l'espace de négociation à l'intérieur duquel devait prendre vie le réseau local que constitue le projet COPRIM<sup>179</sup>. Entité influente du réseau global, elle a rendu nécessaire la participation d'une équipe SHS au projet.

---

<sup>178</sup> Cet extrait est issu d'une enquête qualitative menée dans le cadre d'une réflexion plus large portant sur « l'appropriabilité et l'actionnabilité des études SHS dans le champ de l'innovation technologique » réalisée entre 2008 et 2009 et portée par l'ERT Umanlab. Dix entretiens semi-directifs ont été menés auprès des partenaires de l'ERT, dont le CEA-LETI. Ils ont porté sur les thèmes suivants : définition d'une étude SHS selon les catégories de personnes interrogées, intérêts et limites, rôle et statut dans l'organisation, changements produits par l'apport de connaissances des SHS au sein de l'organisation. Nous utiliserons à plusieurs reprises dans le mémoire des extraits de ces entretiens. Nous remercions Umanlab d'avoir mis ces documents à notre disposition.

<sup>179</sup> L'ANR résume le projet en un titre : « Sciences Exactes et Sciences Humaines au service de la protection de la vie privée » in *Mobilité et Ubiquité : vers le nomadisme numérique*, Les cahiers de l'ANR n°1, juin 2009

## ***B - Observer (quasi) clandestinement une organisation formelle : la participation totale au projet COPRIM<sup>180</sup>***

*« L'observation directe consiste à être le témoin des comportements sociaux d'individus ou de groupes dans les lieux mêmes de leurs activités ou de leurs résidences sans en modifier le déroulement ordinaire. Elle a pour objet le recueil et l'enregistrement de toutes les composantes de la vie sociale s'offrant à la perception de ce témoin particulier qu'est l'observateur. Celui-ci côtoie et étudie les personnes, assiste aux actes et aux gestes qui produisent leurs actions, écoute leurs échanges verbaux, inventorie les objets dont elles s'entourent, qu'elles échangent ou produisent. » (Peretz, 2004 p. 14)*

Nous avons auparavant témoigné de notre volonté de pouvoir suivre les acteurs du projet et de mettre l'accent, dans cette partie de notre analyse, sur le processus méthodologique d'élaboration d'une projection d'usage. Notre démarche d'enquête, qui participe de l'observation directe, nous a conduit à emprunter la voie de la (quasi) clandestinité pour être menée à bien. Nous souhaitons, dans les lignes qui suivent, exposer les tenants et les aboutissants d'une telle posture d'investigation. Ce travail a avant tout pris la forme d'une participation totale telle que définie par Junker :

*« Dans ce rôle, les activités en tant que telles sont complètement cachées. Le chercheur de terrain est ou devient un membre à part entière d'un groupe constitué, partageant ainsi des informations secrètes ignorées des personnes extérieures. Sa liberté d'observer hors du système de relations propres au groupe est limitée [...] Quand le participant apparaît au grand jour comme un chercheur qui fait état de ses observations, il peut s'attendre à passer pour un espion... » (Junker, 1960 p. 35-37 cité par ; Peretz, 2004)*

Afin de mieux saisir les particularités de notre investigation, nous nous inspirons du travail du sociologue Henri Peretz (2004) qui a identifié différentes étapes de la réalisation d'une observation : les relations ainsi que l'entrée dans le milieu, l'établissement dans le milieu et le développement de relations, le recueil de données, la rédaction des notes et enfin le codage et la présentation des résultats.

### **Relations et entrée dans le milieu**

Un an et demi après l'entame de notre travail de recherche, j'étais<sup>181</sup> en quête de matériau empirique complémentaire à ceux déjà disponibles<sup>182</sup> pour étayer l'argument de la

<sup>180</sup> « Dans ce contexte [l'observation à découvert d'une organisation formelle], l'observateur est accepté comme tel au sein d'une organisation sociale régie par des règles formelles et hiérarchisée ; il séjourne au milieu des participants au su et au vu de tout le monde ou presque. » (Peretz, 2004 p. 71)

thèse. La mise à disposition d'un bureau au sein du Laboratoire des IDées (LID) du CEA-LETI me permettait de demeurer à l'affût d'offres de matériaux accessibles et répondant à mes objectifs de recherche. Ainsi, c'est par le détour d'une conversation de couloir avec un membre du LID que j'appris l'ouverture d'un poste d'ingénieur de recherche contractuel auprès de l'ERT Umanlab. La mission à remplir était la suivante :

*« Réalisation d'un état de l'art sur les questions de gestion de la vie privée des utilisateurs de technologies de communication sans contact et identification des pré-requis utilisateurs et recommandations pour l'élaboration des scénarios d'applications des technologies sans contact développées dans le projet COPRIM. »* (Source : contrat de travail)

L'officialisation de mon implication eut lieu la semaine suivant la première réunion plénière du projet, soit le 1er février 2008. La contribution de l'ERT Umanlab au projet relevait ainsi en interne d'une organisation hiérarchique classique : un responsable de projet représentant l'équipe et pilotant le travail effectué, un chargé de recherche assurant la bonne marche du travail opérationnel et encadrant la production de l'ingénieur de recherche, rôle que j'assumais.

Ainsi, j'ai dû prestement endosser l'habit d'expert<sup>183</sup> par-dessus celui de doctorant afin d'accéder au terrain. Autrement dit, les raisons de l'implication tardive d'une équipe experte en « usages » au projet ont paradoxalement contribué à nourrir mes espoirs, en termes de recherche, quant à la richesse escomptée du terrain choisi : « *l'étiquetage* » de l'équipe Umanlab comme experts ainsi que leur implication en dernier recours<sup>184</sup> encourageaient à penser que les débuts du projet puissent être marqués par d'importantes périodes de doute, notamment quant à la définition du rôle d'un partenaire dont l'implication n'était pas évidente au départ.

C'est donc par le biais d'une organisation hiérarchisée (Umanlab) que j'ai pris part au projet, profitant de l'influence de l'ANR pour y associer des SHS. Cette situation de *pièce rapportée* par le financeur du projet compliquait dès le départ la possibilité d'observer à découvert le travail d'élaboration du scénario pour deux raisons essentielles.

D'abord, lors des réunions internes à Umanlab ayant eu lieu autour de la première réunion plénière, le doute l'emportait sur les certitudes quant aux contours exacts du travail

---

<sup>181</sup> L'usage de la première personne du singulier est utilisé à partir d'ici afin de souligner le caractère subjectif des expériences relatées et des conclusions qui en sont tirées. Cet usage sera limité à cette partie.

<sup>182</sup> Voir partie III.

<sup>183</sup> Voir chapitre I.XIII - A -

<sup>184</sup> Voir supra.

à effectuer. La sollicitation précipitée de l'équipe ainsi que la forte coloration technique de l'annexe technique au projet – distribuée quelques jours avant la réunion, rejaillissaient sur le contenu de nos réunions de travail préparatoires : nous luttions alors pour identifier les desseins des initiateurs du projet et partant, pour identifier ce que nous devions y faire. Ainsi, c'est tacitement qu'il fut entendu qu'en raison de la position inconfortable que nous tenions alors, il était exclu d'afficher ostensiblement des prétentions scientifiques qui dépassaient la mission dont nous avions été originellement investis.

A ces écueils à l'établissement d'une observation participante à découvert, s'ajoutait l'inconnue des personnels représentant les équipes partenaires au projet. Aucun des membres de l'équipe Umanlab n'avait connaissance des autres professionnels engagés dans le projet, ce qui réduisait sensiblement les possibilités de compter *a priori* sur le concours de participants-observateurs, comme les décrit Madeleine Grawitz :

*« L'observateur se mêle au groupe et se livre à une observation-participation, mais, en même temps, certains observés lui fournissent de explications et se conduisent comme des participants-observateurs. Ce moyen, fréquemment employé, l'est très spontanément sous la forme : « il est bon d'avoir un allié dans la place. » (Grawitz, 1996 p. 704)*

Cette absence d'alliés potentiels conjuguée à l'indétermination de notre mission ne jouait pas en faveur d'un affichage irrésolu de notre ambition à se servir du terrain à d'autres fins que celles prévues au départ. Le récit de l'établissement dans le projet va confirmer la nécessité d'avancer à visage couvert.

### **S'établir et développer des relations dans le milieu, formes de recueil de l'information**

Comme nous l'avons précédemment annoncé, l'entrée effective dans le projet s'est effectuée lors de la réunion plénière du 1<sup>er</sup> février 2008. Celle-ci s'est faite sans encombre puisque cette réunion consistait en un tour de table de présentation des partenaires au projet ainsi qu'à un rappel des grandes lignes de celui-ci. Le temps dédié à l'observation ainsi que celui dédié à notre participation au projet ont été identiques : durant une période d'environ un an et demi, nous avons activement participé à l'élaboration de scénarios d'usage du dispositif à concevoir. Cependant, en volume, notre travail d'expert a largement débordé sur le temps d'observation nécessaire au recueil de nos données. D'abord, au niveau de la production fournie : hormis le travail d'élaboration des scénarios, nous avons en charge la rédaction d'un état de l'art de la notion de « Privacy » dans les sciences sociales. Par



ailleurs, de nombreuses présentations PowerPoint<sup>®</sup> ont dû être rédigées pour servir de support aux présentations d'avancement de notre travail lors des réunions de projet. Pointer ce déséquilibre nous sert à souligner le fait que cet investissement constituait un gage de clandestinité pour notre observation, tant au niveau des autres parties au projet qu'à l'intérieur de l'équipe SHS à l'égard de laquelle j'adoptais une attitude de plus en plus laconique et vaporeuse sur mes intentions de recherche. Le travail d'observation s'est ainsi cantonné aux moments durant lesquels les scénarios ont fait l'objet de discussions entraînant, ou non, des modifications. On peut distinguer alors :

- les réunions plénières qui constituaient des moments privilégiés et dédiés à la prise de décision collective et à la consolidation des éléments à livrer
- les réunions téléphoniques impliquant l'ensemble ou seulement une partie des partenaires et dédiées à la coordination des travaux en cours
- les réunions préparatoires aux assemblées plénières ou aux rendez-vous téléphoniques qui se déroulaient en interne (Umanlab) ou qui ont associé un partenaire autre que Umanlab et portant sur des points précis des travaux en cours, la somme des échanges informels ayant lieu dans l'environnement du campus Minatec du fait de l'hébergement de Umanlab dans ses locaux
- mais également les emails échangés durant tout le temps de notre observation.

Chacun de ces temps d'observation nous offrait différents types de matériau pour analyser les mécanismes de production de l'usage projeté (voir Tableau 5).

Tableau 5. Lieux de recueil de l'information

Type d'assemblée observée	Objectif	Partenaires Participant	Matériau	Nombre	Durée
Réunions plénières	Prise de décision collective Consolidation des livrables	Tous	Scénarios en construction Objets intermédiaires de conception Verbatim Notes	(tous les trois mois)	Une journée
Réunions téléphoniques	Coordination des travaux en cours	Tous	Scénarios en construction Objets intermédiaires de conception Verbatim Notes		Une à trois heures
Réunions préparatoires	Travail sur des points de détails Préparation de réunions plus générales	Umanlab + un ou deux partenaires	Scénarios en construction Objets intermédiaires de conception Verbatim Notes	14	Une demi-journée à une journée
Echanges informels	--	--	Emails Entretien informel	--	--

Nous avons assisté à l'ensemble de ces événements en qualité de représentant de l'expertise portée par Umanlab et notre qualité de doctorant n'a été évoquée que lors du recensement des ressources humaines exigé par l'ANR (sept mois après le lancement du projet) ainsi que lors d'échanges informels avec l'un des employés du partenaire industriel, également en formation doctorale (cryptologie). Il est à noter que le travail de lecture et d'appropriation des enseignements de la sociologie des usages effectué durant ma première année de thèse

avait grandement facilité ma prise de poste en tant qu'expert, ma « *présentation de [m]oi* » comme telle (Goffman, 1973). Certes, l'équipe-projet, en m'assignant la capacité d'expert, reconnaissait déjà la légitimité de ma présence dans le groupe ainsi que mon aptitude à représenter le « social<sup>185</sup> ». Cependant, mon inexpérience dans le domaine du travail de projection d'usage, m'obligeait à veiller à ne jamais perdre la « *face* » durant les phases d'interactions dans lesquelles je me trouvais pris. Dès lors, j'avais développé un véritable « *appareillage symbolique* » sensé contrevenir à l'apparition de toute « *fausse note* » me démasquant en tant qu'expert ou pire en tant qu'observateur. Ainsi, publiquement, j'alignais mon vocabulaire sur celui employé par le responsable projet, rompu au jargon de la sociologie des usages appliquée à l'innovation, je ressassais mes notes de lecture pour être à jour lors des discussions internes, je prenais note de tous termes et expressions techniques et m'empressais d'en découvrir les définitions, me présentais en déclinant rapidement mon prénom et mon nom, celui de mon employeur, ma formation académique, mes centres d'intérêts professionnels ainsi que ma raison d'être dans le projet, comme il est d'usage dans ces projets. En somme, comme le résume Goffman, je pris à cœur le rôle d'expert puisque la situation d'observation, pour être sauvegardée, l'exigeait :

*« Jouer un rôle, c'est donc s'accorder des libertés mineures, mettre la tête hors de l'eau un instant pour s'étirer ou s'excuser. Ces petits abandons de soi sont l'ombre de nos actions, à peine perceptibles, et la sociologie a sans doute tout fait, et depuis longtemps, pour les ignorer. Qu'un comédien doive s'interdire ce genre d'écarts lorsqu'il interprète un rôle (sauf s'ils sont programmés comme tels) devait attirer l'attention sur eux et nous porter à comprendre plus clairement que, si l'univers social est fait de rôles interprétés par des personnes, ces personnes ont le droit d'exister par ailleurs et sont confirmées dans ce droit. »* (Goffman, 1991 p. 536)

Au-delà de l'incertitude qui planait sur ma capacité à endosser ce rôle, le statut octroyé d'expert a, semble-t-il, rendu « *invisibles* » certains éléments personnel de ma « *face* »<sup>186</sup> dont j'appréhendais qu'ils jurent avec le « *décor* » du projet. Ainsi en a-t-il été de ma tenue vestimentaire (décontractée, bigarrée) pouvant, au regard de l'austérité en vigueur

<sup>185</sup> « La reconnaissance sociale dans le milieu professionnel semble pallier le manque de reconnaissance et de définition institutionnelle. Il existe des degrés de reconnaissance selon le statut du praticien. Etre identifié comme sociologue est plus fréquent dans les environnements salariaux et organisationnels (hiérarchie, collègue) que dans l'environnement du travail indépendant (clients). [...] La reconnaissance sociologique dans le milieu se double d'une reconnaissance et d'une définition sociologique dans la discipline. Les praticiens de la sociologie se sentent sociologues parce qu'ils ont acquis des connaissances sociologiques, hérité d'un ensemble de savoir être, d'habitudes de pensée et d'attentes vis-à-vis de leur fonction qu'ils jugent ancrée dans la tradition sociologique. [...] Cette logique « culturelle » de l'identification de soi se nourrit d'un désir de définition sociologique qui consolide le lien avec la sociologie scientifique. » (Pirou, 2006 p. 42-43)

<sup>186</sup> Jean Nizet et Natalie Rigaux traduisent « façade » comme cet élément ayant pour fonction de « fixer la définition de la situation [qu'un acteur] tente de donner. » (Nizet & Rigaux, 2005 p. 21)

lors de ces projets (pantalon de ville, chemise unie), être considérée comme excentrique. Cependant, elle n'entrait pas nécessairement en conflit avec la réputation d'originalité qu'ont les sociologues<sup>187</sup> praticiens, au moins à l'intérieur du CEA-LETI<sup>188</sup>. Concernant mon âge, j'ai été invariablement le cadet des participants réguliers aux réunions sans que cela n'ait fait l'objet d'aucune remarque ou attitude en ce sens. Aussi, mes caractéristiques ethniques (type africain) ne sont jamais intervenues comme élément pesant dans le déroulement de l'interaction. Il faut enfin noter qu'à l'exclusion de trois comités de pilotage et deux réunions téléphoniques, l'ensemble des participants étaient de sexe masculin. Ainsi, le « *décor* » installé par le projet, en m'attribuant un statut d'expert en sciences sociales, a contraint autant mes manières de faire qu'il autorisait l'expression d'une certaine forme d'exotisme notamment due aux présomptions pouvant peser sur les SHS vues du monde technologique. En somme, le travail de « *démonstration*<sup>189</sup> » de mon expertise a encouragé le passage sous silence de mon entreprise d'observation. Nous aborderons dans la sous-partie suivante plus précisément les tensions qui ont pu naître de l'endossement de ces deux rôles.

### ***C - Questions de distance réflexive au terrain***

*« Faute de pouvoir s'en tenir à ce qu'il sait, l'expert se prononce au titre de la place que sa spécialité lui a value. Par là, il s'inscrit et il est inscrit dans un ordre commun où la spécialisation a valeur d'initiation en tant que règle et pratique hiérarchisante de l'économie productiviste. Pour s'être soumis avec succès à cette pratique initiatique, il peut, sur des questions étrangères à sa compétence technique mais non pas au pouvoir qu'il s'est acquis par elle, tenir avec autorité un discours qui n'est pas plus celui du savoir mais celui de l'ordre socio-économique. Il parle en homme ordinaire, qui peut « toucher » de l'autorité avec du savoir comme on touche sa paie pour du travail. Il s'inscrit dans le langage commun des pratiques, où d'ailleurs une surproduction d'autorité entraîne sa dévaluation*

<sup>187</sup> Par commodité, et en référence à la « sociologie des usages », nous emploierons le terme « sociologue » pour désigner les membres de l'équipe Umanlab, ce malgré leurs parcours éclectiques.

<sup>188</sup> Durant ma période d'hébergement au LID, j'ai eu l'occasion de le constater durant de nombreuses discussions informelles avec les équipes techniques du CEA-LETI, les remarques apportées pouvant être positivement ou négativement connotées. A titre d'exemple, l'un des techniciens de laboratoire avec qui j'entretenais des rapports cordiaux nous avait attribué le doux sobriquet de « poètes du dimanche » tandis que lors de la diffusion électronique d'une soutenance de thèse en SHS, un ingénieur répondit à l'ensemble des destinataires du mail par un message contenant un lien vers un site affichant en page d'accueil une énorme image de feuille de marijuana...

<sup>189</sup> « La question n'est pas de savoir s'il faut masquer ou non l'identité du sociologue mais de comprendre par quels mécanismes passe sa reconnaissance. L'un de ces mécanismes semble relever de la *démonstration*. Le sociologue doit faire la preuve de l'utilité de ses compétences, condition *sine qua non* de l'acceptation, par les partenaires, de sa compétence sociologique. » (Bretagne, 2004 p. 154)

*puisqu'on s'en procure toujours plus avec une somme égale ou inférieure de compétence. Mais lorsqu'il continue à croire ou à faire croire qu'il agit en scientifique, il confond la place sociale et le discours technique. Il prend l'un pour l'autre : c'est un quiproquo. Il méconnaît l'ordre qu'il représente. Il ne sait plus ce qu'il dit. Certains seulement, après avoir longtemps cru parler comme experts un langage scientifique, se réveillent de leur sommeil et s'aperçoivent soudain que, depuis un moment, tel Félix le chat dans le film d'antan, ils marchent en l'air, loin du sol scientifique. Accrédité par une science, leurs discours n'étaient que le langage ordinaire des jeux tactiques entre pouvoirs économiques et autorités symboliques. » (De Certeau, 1990 p. 22-23)*

L'introduction de cette critique acerbe de Michel de Certeau de l'expertise vise, dans notre exposé, moins à discuter la scientificité de la production des sociologues praticiens<sup>190</sup> qu'à jeter les bases d'un examen réflexif des tensions qui ont traversé mon travail tout au long de la période d'investigation. Un rapide détour biographique se révèle ici utile à la compréhension du phénomène contre lequel j'ai dû lutter : *l'aspiration par le terrain*<sup>191</sup>. Après de brèves études de droit, j'ai intégré l'Institut d'Etudes Politiques de Grenoble, période durant laquelle j'ai effectué un second cycle professionnalisant (master II) destiné à former des futurs cadres spécialistes des études d'opinion et des études de marché. Le type de profil que je présentais alors coïncidait avec celui recherché pour occuper le poste de doctorant pour la présente thèse. Cependant, s'il m'a fallu entamer un travail d'initiation aux rites et aux codes en vigueur dans le monde de la recherche académique, celui-ci ne s'est pas accompli par le biais d'une formation préparatoire au doctorat (master recherche) mais a eu lieu parallèlement à mon travail d'investigation par le biais de formations doctorales, de l'encadrement de mon travail et bien entendu, de l'investissement personnel. Le rappel du contexte d'entrée dans la recherche permet d'appréhender le poids important des « *partenaires silencieux*<sup>192</sup> » dans mes difficultés à *sortir* du terrain. Ma formation académique initiale, privilégiant en bout de course l'efficacité pragmatique à la réflexivité scientifique a, d'une certaine manière, contribué à forger mon « *conditionnement culturel et social* » (Grawitz, 1996 p. 301), entravant ce faisant l'expression d'un discours savant sur une pratique dont j'étais moi-même sujet/objet. En réalité, non seulement j'adhérais tacitement dans les vertus et la légitimité de l'entreprise de mise à disposition des SHS comme aide à la prise de décision, mais j'étais paradoxalement incapable de voir cette prise

<sup>190</sup> Encore une fois, l'accent est porté plus sur ce qu'ils font (lors de la mise en place de l'usage projeté) que sur ceux qu'ils sont (au regard d'une sociologie plus académique).

<sup>191</sup> Je remercie Clémence Emprun pour cette expression (Laboratoire C2SO/ ENS Lyon)

<sup>192</sup> « Background assumptions provide some of the bases for choice and the invisible cement for linking together postulations. From beginning to end, they influence a theory's formulation and the research to which it leads [...] Theories are accepted or rejected because of the background assumptions embedded in them » (Gouldner, 1970 p. 29)

de position comme telle. En ce sens, si l'on peut admettre qu'idéalement et pris isolément, les acteurs du projet se fondent sur des travaux scientifiques, leur activité de collaboration fait place honorable au déploiement de « *logiques pratiques*<sup>193</sup> ». C'est à cet endroit que la singularité de ma position était criante : mon inexpérience en la matière ainsi que ma relative ingénuité scientifique renversaient les biais identifiés par Bourdieu dans l'élaboration d'un rapport savant à la pratique (Bourdieu, 1980). Dans *Le sens pratique* (1980), Bourdieu met en garde le savant d'une part, contre la tentation d'amputer la pratique de tout élément logique, fut-ce-t-il non scientifiquement fondé ; d'autre part, le sociologue condamne l'absence de prise en compte du contexte de ces pratiques par l'opération de qualification de celles-ci au regard de grilles de catégorisation exclusivement savantes. Or, par jeu de miroir, et avec toute la modestie que peut supporter la comparaison, je me trouvais aux antipodes de la position de chercheur affirmé : c'est la « *logique pratique* » qui me paraissait la plus familière, la moins questionnable dans sa cohérence tandis que les grilles de lecture, d'analyse et donc de catégorisation scientifiques ne s'imposaient pas. Cette situation renversante paralysait sèchement les éventualités d'émergence de toute rupture épistémologique du fait de la substitution sourde de l'expertise, comme logique pratique, à l'étrangeté de la relation à l'objet scientifique, inversant mais n'invalidant pas le constat de Pierre Bourdieu :

« *La relation pratique que l'ethnologue entretient avec son objet, celle de l'étranger, exclu du jeu réel des pratiques sociales par le fait qu'il n'a pas sa place – sauf par choix et comme par jeu – dans l'espace observé et qu'il n'a pas à s'y faire une place, est la limite et la vérité de la relation que l'observateur, qu'il le veuille ou non, qu'il le sache ou non, entretient avec son objet : le statut de spectateur qui se retire de la situation pour l'observer implique une rupture épistémologique, mais aussi sociale, qui ne gouverne jamais aussi subtilement l'activité scientifique que lorsqu'elle cesse de s'apparaître comme telle, conduisant à une théorie implicite de la pratique qui est corrélative de l'oubli des conditions sociales de l'activité scientifique.* » (Bourdieu, 1980 p. 57)

Plusieurs éléments m'ont cependant rappelé à la nécessité de résoudre cette tension. Tout d'abord, le contexte de l'activité de conception. Le caractère exploratoire de la démarche tout autant que les qualités des partenaires, notamment le CEA-LETI et l'UVSQ,

---

<sup>193</sup> « Il faut reconnaître à la pratique une logique qui n'est pas celle de la logique pour éviter de lui demander plus de logique qu'elle n'en peut donner et de se condamner ainsi soit à lui extorquer des incohérences, soit à lui imposer une cohérence forcée. [...] Cette *logique pratique* – au double sens du terme – ne peut organiser toutes les pensées, les perceptions et les actions au moyen de quelques principes générateurs étroitement liés entre eux et constituant un tout pratiquement intégré, parce que toute son économie, qui repose sur le principe de l'économie de logique suppose le sacrifice de la rigueur au profit de la simplicité et de la généralité [...] » (Bourdieu, 1980 p. 144)

encourageaient ces derniers à s'appuyer sur la littérature scientifique pour argumenter de leurs positions. Ainsi, j'observais les partenaires techniques effectuer des allers-retours constants entre propositions technologiques, faisabilité technique et état de l'art scientifique. Cette indivision du travail pratique se retrouvait également dans une partie de notre propre travail. L'état de l'art que nous avons rédigé sur la notion de « Privacy » en SHS intégrait quasi indistinctement références théoriques, savoirs actionnables et préconisations pragmatiques. Il ne constituait en réalité pas plus que la production d'un sociologue praticien sinon qu'en sus d'une forme d'imagination sociologique et d'une prise en compte des préoccupations des acteurs concernés<sup>194</sup>, l'établissement d'une troisième limite s'avérait nécessaire à l'activité du travail d'observation : la défamiliarisation avec cette première production qu'était l'état de l'art. Ce processus, nécessaire à « *l'objectivation de l'objectivation* » (Bourdieu, 1980), a été enclenché du fait de l'intervention d'une externalité positive quasi hasardeuse : l'un des membres de l'équipe Umanlab, une fois le document achevé, s'est enquis du statut de celui-ci et des possibilités de valorisation académique de cette production. Sans qu'il soit nécessaire de rendre compte ici du contenu des discussions ayant eu lieu autour du problème soulevé, le seul fait de poser ce problème comme tel a permis le rétablissement de la tension entre activité d'expert et travail d'observation, la première alimentant le second. Cette tension pouvait se comprendre par le retour aux fondements de ce travail de thèse qui, comme travail de recherche, consiste, comme le dirait Michel Callon, à représenter des entités nouvelles à partir de la création d'entités nouvelles, ou autrement dit à produire le texte d'un texte :

*« Les sciences sociales ne sont ni moins productives ni moins imaginatives que les sciences de la vie. Avec ces dernières elles contribuent à la prolifération d'entités qui composent notre monde commun et au nom desquelles elles prennent la parole. Cette vision du travail de recherche comme performance est évidemment à l'opposé des réalismes simples qui considèrent qu'il existe quelque chose qu'on appelle société et qui existe à distance du chercheur et dont il s'emploie à découvrir les règles de fonctionnement. Le sociologue ne dévoile pas : il représente, et son succès dépend de sa capacité à rendre robustes ses représentations. L'obtention de cette robustesse n'a rien à voir avec l'habileté rhétorique, elle suppose la mise en place d'équipements, d'outils qui parviennent à rendre*

<sup>194</sup> « Afin d'apporter un nouveau regard sur le problème posé, le sociologue praticien réalise un travail scientifique d'aller-retour constant entre la réalité sociale qu'il observe, l'analyse de la perception qu'en ont les acteurs et les théories qu'il mobilise pour l'éclairer. C'est une compétence que le praticien doit posséder s'il veut comprendre les enjeux sous-jacents à la demande et mener l'intervention à ses fins. [...] Ce travail d'analyse distanciée passe par au moins deux démarches conjointes de réflexion. La première concerne la prise en compte de l'environnement et l'analyse de la structure sociale. Elle fait appel à « l'imagination sociologique » décrite par C. Wright Mills (1971). La seconde passe par l'analyse et la confrontation des points de vue de l'ensemble des acteurs concernés par la demande. » (Legrand, 2004 p. 96)

*durables les entités représentées : celles-ci, et c'est en cela que consiste l'effet de réalité, participent à la fabrication de leur propre identité à travers les instruments mobilisés (cette remarque est vraie à la fois pour les neutrinos ou pour les ainsi nommés exclus). » (Callon, 1999 p. 68)*

En somme, la mise en abîme devait sans cesse être rendue prégnante pour distinguer l'objet du sujet, pour ne se poser la question de la qualification normative du travail d'expertise – science ou pas science. Ce « *Boundary work* » (Gieryn, 1983) n'était pas notre objet, et notre engagement, tout réduit qu'il puisse être à des jeux tactiques entre pouvoirs économiques et autorités symboliques, devait périodiquement mais agilement s'estomper pour rentrer dans le temps de la science :

*« Il y a un temps de la science qui n'est pas celui de la pratique. Pour l'analyste, le temps s'abolit : non seulement, comme on l'a beaucoup répété depuis Max Weber, parce que, venant toujours après la bataille, il ne peut avoir d'incertitude sur ce qui peut advenir, mais aussi parce qu'il a le temps de totaliser, c'est-à-dire de surmonter les effets du temps. La pratique scientifique est si détemporalisée qu'elle tend à exclure même l'idée de ce qu'elle exclut : parce qu'elle n'est possible que dans un rapport au temps qui s'oppose à celui de la pratique, elle tend à ignorer le temps et, par là, à détemporaliser la pratique. Celui qui est engagé dans le jeu, pris par le jeu, s'ajuste non à ce qu'il voit, mais à ce qu'il prévoit, à ce qu'il voit à l'avance dans le présent directement perçu, passant la balle non au point où se trouve son partenaire mais au point que celui-ci atteindra – avant l'adversaire – dans un instant, anticipant les anticipations des autres, c'est-à-dire, comme dans la feinte, qui vise à les déjouer, des anticipations d'anticipations. [...] C'est seulement pour qui se retire du jeu complètement, qui rompt totalement le charme, l'illusio, renonçant à tous les enjeux, c'est-à-dire à tous les paris sur le futur, que la succession temporelle peut apparaître comme pure discontinuité et que le monde peut se livrer dans l'absurdité d'un présent dépourvu d'a-venir, donc de sens, à la façon des escaliers ouvrant sur le vide des surréalistes. Le sens du jeu est le sens de l'à-venir du jeu, le sens du sens de l'histoire du jeu qui donne son sens au jeu. » (Bourdieu, 1980 p. 137-138)*

La superposition de ces deux temps dans notre cas, ainsi que leur distinction, ont également été facilitées par la dissimulation de mes activités d'observation auprès des partenaires. De la sorte, je prémunissais les contagions de la « *logique pratique* » à la « *logique logique* » et assumais de sacrifier une forme d'honnêteté ou de probité sur l'autel de la recherche. Dans la veine de Michel Callon qui, pour expliquer son échec à être entendu comme rapporteur général adjoint du Colloque national « Recherche et Technologie »,



organisé par Jean-Pierre Chevènement, rapportait son inexpérience, sa jeunesse, son isolement et le manque d'incorporation de ses analyses sociologiques dans des instruments visibles (1999), nous avons considéré l'engagement dans l'élaboration de l'usage projeté comme mode de participation et comme condition de réalisation de l'observation<sup>195</sup>.

Cela affirmé, reste irrésolue la question morale ou politique, ou autrement dit la posture du sociologue dans sa collaboration au pouvoir technico-économique. Pour traiter cette question, nous référons à certains débats ayant agités la communauté de la sociologie des sciences et des techniques. Le constructivisme social a notamment été l'objet de critiques considérant que ses tenants se cachaient derrière le voile de la neutralité axiologique pour ne pas dire les valeurs qui supportaient leurs énoncés (Giere, 1993 ; Winner, 1993) ou de manière plus mesurée de ne pas être en mesure d'apporter de réponse systématique aux questions normatives soulevées dans leurs recherches (Radder, 1996 ; Hamlett, 2003). Notre engagement sur le terrain ne doit pas être associé à une forme d'engagement politique comme le désire Fuller :

*« If sociologists and other students of actual practice wish their work to have the more general significance that it deserves, then they should practice some 'naturalistic epistemology' and welcome the opportunity to extrapolate from is to ought. »* (Fuller, 1988 p. xi)

Seule la motivation de *faire* de la recherche a participé de notre entreprise avec celle d'avoir l'opportunité de pouvoir observer et analyser un objet qui, intuitivement, nous paraissait original. Dès lors, la question de l'instrumentation politique des sciences sociales – qu'elle soit posée à travers la collaboration de praticiens avec le CEA-LETI ou alors par le biais de notre propre engagement, pour intéressante qu'elle soit, n'a que peu ou prou influencé notre démarche sauf à considérer l'accueil sceptique dont nous avons pu faire l'objet auprès de certains publics hostiles à ce genre d'alliances (voire partie I). Ainsi, et quitte à n'être pas en phase avec le vent de critiques portées au constructivisme social, nous tenions à ce que ce travail puisse s'insérer dans une entreprise de recherche de vérité et de ce

---

<sup>195</sup> « On a beaucoup trop sous-estimé, me semble-t-il, l'importance et le rôle joué par les instruments qu'ont élaboré les sociologues au cours du temps. Des apports de la sociologie, on ne retient bien souvent que les concepts et les cadres théoriques. Pourtant, à l'instar de toutes les autres disciplines, l'essentiel des effets produits par la sociologie est passé et passe par les instruments, méthodes, dispositifs d'observation que les chercheurs ont élaboré et par les activités de formation qu'ils ont mises en place. Envisagé dans cette perspective on peut dire que la sociologie a réussi au-delà de tout espoir. On ne peut plus interviewer un acteur sans tomber sur des outils et par conséquent des modes de raisonnement qui à un moment ou un autre ont été conçus, testés, transportés, inculqués par des sociologues. Nos sociétés sont sociologisées de part en part, grâce à la dissémination des méthodes et des instruments utilisés pour produire des données qui, en retour, c'est une dette acquittée, facilite la poursuite du travail sociologique [...]. Enquêtes, questionnaires, analyses factorielles de correspondance, sondages, analyses statistiques, tables de mobilité il faudrait une bibliothèque pour recenser ces outils qui font plus que dire la société, puisque, utilisés en permanence par les acteurs eux-mêmes, ils la mettent en forme, la composent, la structurent et par voie de conséquence influencent fortement le cours des actions. » (Callon, 1999 p. 70)

fait, sans nier l'improbabilité d'une posture absolument objective, travailler à s'en approcher au maximum, notamment par ce travail de révélation des tensions entre engagement dans le terrain et distance réflexive nécessaire au travail de recherche (Anjembe, Michalon & Emprun, 17 novembre 2009). Enfin, en nous engageant dans ce terrain, nous désirions aussi emprunter le chemin de l'humilité quant aux mondes observés. Doublement novices, cela nous prévenait de considérer les acteurs et leurs savoirs avec condescendance tout en reconnaissant la valeur de la matière rendue disponible par les interactions que leurs présences nous offraient, comme en témoigne Antoine Hennion, en réflexion sur son concept de « *création*<sup>196</sup> ».

---

<sup>196</sup> « The concept of creation that we have defended has as a corollary the necessity of radically questioning another « natural » frontier, that which separates the sociologist from the actor. Far from being a blemish in our measurements, observers and their interaction with what they observe is the only way that we have of knowing-via feeling reactions to them. We ourselves create the barriers that prevent us from thinking about creation. If, in my example of the song, music is to one side, obedient to the laws of a rigidly hierarchical language (look in the musicology section of a bookstore) and if the lyrics are on the other, with their rhymes and reasons (see the semiology section), if we turn to yet another vocabulary (mythology, mass psychology, rites, the imagination) to describe the scene and its collective workings, while sociology takes on the strategy of the actors and the determination of tastes, then no concept we use has the slightest chance of being strong enough to encompass trees with such a huge trunk and such distant roots. Yet these distances do not exist when the actor/operators construct their own experiences of the real. It conjures a fantasy of a microscope: I, sociologist, observe you. Whatever may be the sympathetic links that have allowed me to feel the forces that bear down on you, as soon as I turn my back, I reconstruct our relationship by crushing you between two slides. All you are now is microbes unaware of your own movements. Luckily, I am there to describe you to my colleagues. No, it is another ball game when the sociologist comes to share the daily work of the « professional. » Ignorant sociologists have listened to knowledgeable actors speak of relationships known only to them- since they are the only ones who bring them into play. They are knowledgeable about their acts and are the actors of a form of knowledge. We should not take revenge for our initial ignorance by transforming those who know more than we do into guinea pigs. The distribution of forces between observer and observed changes continually according to where we are. If we multiply our visits, we become knowledgeable with respect to others. We knit our own written network, we cut off, we approach, we regroup. We produce text; others produce music, science, or innovations. That gives us no right to create an impassable barrier along a road we have traveled a thousand times, in both directions if we have done our work well-the road between the place of the learned and that of the ignorant. » (Hennion, 1989 p. 422)

## VIII - Conclusion de la partie II

---

En définissant plus précisément les contours des notions de scénario et de scénarisation, nous pouvons désormais modifier la substance de notre définition provisoire. Nous avons jusqu'ici considéré la projection d'usage comme un *travail de représentation de l'usage de la technologie*. L'utilisation faite des scénarios, indépendamment de leurs différents régimes esthétiques ou ontologiques, nous amène à considérer ceux-ci, et par extension, la projection d'usage, comme la *représentation d'écologies socio-technique de l'usage*.

L'usage du terme écologie (Golfin, 1972) s'explique par le fait que bien que les concepteurs de scénario tendent à insérer l'usage dans des situations où l'interdépendance des éléments socio-techniques assure la stabilité ou l'instabilité d'une écologie, il est impossible pour eux de réaliser un véritable cadre de référence socio-technique. La prépondérance d'une vision systémique, voire fonctionnaliste, du fonctionnement des communautés et des sociétés humaines ainsi que la volonté d'en améliorer l'organisation ou l'équilibre traversent l'ensemble des types de scénarios abordés. Dans la définition provisoire, la projection d'usage faisait la part belle à l'usage, dans la lignée de la carrière du concept (voir Partie 1). Cependant, l'usage est mis en lumière comme une composante d'une écologie le dépassant, celle des cadres de fonctionnement de la solution technologique. Aussi, bien qu'il puisse paraître évident au sociologue des sciences et des techniques qu'une telle écologie ne pourrait être technique ou sociale par exclusive, il nous a semblé important d'insister sur le caractère mixte de celle-ci. Cette précision permet d'évacuer les écologies fondées sur des équilibres dont l'exclusion de « l'homme » ou de la « technique » sont revendiquées ou sont présentes bien qu'impensées.

Enfin, l'évacuation du terme travail vise à ne pas écarter de la définition de la projection d'usage le produit même du travail effectué. En lui préférant l'utilisation seul du terme représentation, qui renvoie autant à l'action de représenter qu'à la représentation elle-même, nous soulignons l'impossibilité d'appréhender distinctement le processus et le produit de ce processus. Dans un souci de clarté descriptive et de commodité analytique, chacune des parties suivantes de la thèse privilégie soit l'étude du produit de la projection (Partie 3) soit celle de son process (Partie 4), sans toutefois exclure la perméabilité de ces deux éléments dans l'analyse. Il s'agira, conformément à notre intention initiale, de *décomposer* le composite de la projection d'usage en s'intéressant à l'objet scénario en tant

que objet de représentation et aux actions, dynamiques, systèmes de normes et règles opératoires à l'œuvre durant sa conception.

## **Partie 3. Le scénario, investissement de forme fictionnelle**

*« Les conquérants savent que l'action est en elle-même inutile.  
Il n'y a qu'une action utile, celle qui referait l'homme et la terre.  
Je ne referai jamais les hommes.  
Mais il faut faire « comme si ».*  
*Camus A. (1942). Le mythe de Sisyphe, Paris, Gallimard, p.142*

Nous souhaitons désormais nous pencher sur le produit de la projection d'usage opérée par l'équipe de conception : le scénario, en tant que « *premiers efforts de matérialisation de l'invention par les mots et les images.* » (Gentès, 2008 p. 88). Dans notre cas d'espèce, l'objet produit a pris la forme finale d'un document de 39 pages coécrit par l'ensemble des partenaires et diffusé dans leur structure et auprès de l'Agence Nationale de la Recherche. Rédigé en anglais, il a pour nom « Scenario specifications » et est structuré de la manière suivante :

- Pages 1 à 3 : page de titre, restriction de la diffusion, historique des versions et mots-clés
- Pages 4 à 7 : table des matières et glossaire
- Pages 8 à 11 : exposé de la méthode d'analyse des scénarios
- Pages 12 à 34 : description et analyse des scénarios
- Pages 35 à 36 : conclusion de l'analyse
- Pages 37 à 39 : annexes

En analysant ce document, nous poursuivons deux objectifs. D'abord, nous souhaitons donner à voir au lecteur un exemple détaillé de production de projection d'usage. Aussi, il s'agit surtout de développer une analyse de la portée symbolique de cette production. Notre objectif est de défendre l'idée que l'enjeu de véridiction qui sanctionne la production scientifique finale est précédé, préparé<sup>197</sup> par *l'investissement de forme fictionnel* qu'est le scénario. Dans les deux chapitres suivants, nous allons démontrer que le scénario est :

- (1) un « *investissement de forme* » (Thévenot, 1986) destiné à rendre disponible pour un transport le travail effectué. La forme produite traduit la mise en équivalence de choses, d'entités ou d'actions différentes, asynchrones ou ayant lieu à des endroits différents. Ces investissements<sup>198</sup> permettent de dégager de leurs contingences ces situations pour les rendre disponibles, compréhensibles et exploitables dans d'autres situations. Dans notre cas d'espèce, le travail effectué par les différents acteurs du consortium doit pouvoir être approprié *a minima* par l'ANR et au mieux par tout membre intéressé de la communauté scientifique. Le scénario est un investissement matériel complémentaire au travail effectué.

---

<sup>197</sup> Voir également Partie 4

<sup>198</sup> « Ainsi, si nous nous sommes attachés au concept d'investissement, c'est parce qu'il pouvait conduire à une formulation plus générale qui relie un coût ou un sacrifice immédiats à un accroissement d'une capacité à assurer la validité (en l'occurrence temporelle) d'une relation. Cette formule d'économie peut en effet nous permettre d'analyser le rapport entre des formes durables, comme celles durcies dans des outillages et résultant d'opérations d'investissements au sens strict du terme, avec d'autres formes également durables, établies dans un cadre juridique notamment, mais aussi à envisager d'autres modalités de généralité qui ne soient pas temporelles (comme celles attachées aux objets dits sociaux). » (Thévenot, 1986)

- (2) Le retour sur investissement<sup>199</sup> attendu est celui de l'intéressement ou de l'enrôlement des commanditaires ou des publics ciblés en s'assurant de la transmissibilité, de la crédibilité et de la force de conviction de la projection d'usage
- (3) L'adhésion escomptée est obtenue par le déploiement d'actes de langage (Austin, 1970 ; Searle, 1972) et d'actes de croyance propre au genre fictionnel. En effet, l'une des caractéristiques majeures de la fiction est que celle-ci repose sur l'impératif d'adhésion à la vraisemblance qui correspond non seulement à un acte de langage mais aussi à un acte de croyance provisoire (Mercier, 2009). L'acte de langage permet de *projeter* le scénario d'usage au-delà de l'ici et du maintenant (Chapitre IX) tandis que l'acte de croyance fonde la légitimité d'une vision du monde (Chapitre X).

Pour ce faire, nous considérons une appréhension large du scénario. Si la tentation est grande de ne s'intéresser qu'au cœur du récit – celui où l'écologie socio-technique est la plus visible, il nous est paru important de ne pas limiter l'analyse aux catégories définies par les acteurs. Ce qui est nommé scénario par eux ne peut être étudié sans aborder les autres matériaux satellites, c'est-à-dire sans introduire dans l'analyse le paratexte qui accompagne le document. En effet, si l'on pousse la comparaison à l'analyse filmique, un film ne saurait être exclusivement analysé à partir du synopsis ou du récit le structurant. Font également partie de la chair du film, les génériques de début et de fin, la bande sonore, la lumière, le montage, voire les salles dans lesquelles il est projeté. Il en est de même pour le scénario.

---

<sup>199</sup> La rentabilité de l'investissement se constate par la comparaison entre le coût de celui-ci (en temps ou en énergie dépensée) et à la validité du résultat escompté. L'investissement est donc rentable lorsqu'il y a « *accroissement d'une capacité à assurer la validité (en l'occurrence temporelle) d'une relation.* » (Thévenot, 1986)



## IX - Le scénario, acte de langage

---

L'objectif d'analyser ce document comme un ensemble d'actes de langage participe de deux raisons. D'une part, en lignée avec la pragmatique linguistique, il s'agit de rejeter les actes de langage qui constituent le scénario comme une simple description du monde, fut-il à venir. D'autre part, cette affiliation permet de rendre compte de l'essence fictionnelle de la projection d'usage et de ses conséquences. En effet, les scénarios permettent aux concepteurs de répondre à (et de se poser) un nombre de questions utiles à l'avancée du processus de conception (Bodker, 1998) : quel est le produit de l'usage pour l'ensemble des acteurs impliqués ? Où se situe l'usage ? Par qui et à quel moment se déclenche-t-il ? Par quels moyens et de quelles manières ? Les scénarios, qui ne représentent qu'un mode de réponse parmi d'autres<sup>200</sup>, ont, à la différence des prototypes, des représentations *ad hoc* ou des méthodes formalisées<sup>201</sup>, la particularité d'être structurés par une trame narrative.

Cette trame et les réponses attendues participent de ces « *tests prospectifs* », durant lesquels une technologie, encore en conception, est soumise à l'épreuve d'un usage généralisé<sup>202</sup> (Pinch, 1993). La particularité de ces épreuves est qu'elles relèvent d'un processus de projection qui établit une « *relation de similarité* » entre, d'une part, les résultats obtenus grâce à l'environnement artificiellement créé pour l'investigation, et d'autre part, les réactions suscitées par l'introduction de la technologie *into the wild*, dans un environnement réel<sup>203</sup>. Cette relation de similarité, qui brouille les pistes entre ce qui est acquis et ce qui est à conquérir, s'obtient par l'élaboration d'outils de régulation du sens inscrits dans les projections.

Ces outils permettent de substituer *la quête du vraisemblable à celle de la vérité*. L'opportunité de l'arbitrage entre le vrai et le faux, le réel et l'imaginé est ce faisant anéantie. Le scénario s'impose comme un récit hybride empruntant au réel, au vrai, au possible et à l'envisageable, pour s'inscrire dans une logique fictionnelle de la vraisemblance. C'est par cette conquête de la vraisemblance que l'extrapolation de la projection et des travaux qui en découleront est crédibilisée. En s'abstrayant du particulier, en atteignant une représentation et une interprétation générales des événements et des

---

<sup>200</sup> Voir partie 2

<sup>201</sup> Voir partie 2

<sup>202</sup> Voir introduction

<sup>203</sup> « The act of projection – whether from the present to the future, from the present to the past, from the particular to the general, from the small to the large, or from the large to the small (as in miniaturization) – depends crucially upon the establishment of a similarity relationship. It is assumed that the state of affairs pertaining to the test case is similar in crucial respects to the state of affairs pertaining to the actual operation of the technology. [...] It is the assumption of the similarity relationship that enables the projection to be made and that enables engineers warrantably to use the test results as grounds that they have found out something about the actual working on technology. » (Pinch, 1993 p. 29)

actions qui prennent figure d'exemple ou de modèle (Mercier, 2009) – en somme, par la fiction, le récit s'inscrit dans une mécanique de l'intéressement.

Dans les quatre sous-parties suivantes, nous allons tenter de démontrer que, non seulement la projection d'usage obéit aux normes de la fiction, mais surtout qu'elle tire de cette conformité sa puissance d' enrôlement. En effet, pour que la fiction fonctionne, il faut que le monde qu'elle offre soit crédible ou recevable aux yeux du lecteur. C'est là que la vraisemblance joue un rôle clé car elle porte un enjeu d'adhésion qui s'exprime par quatre idéaux-types en relation dans l'espace de la fiction. Nous verrons que chacun de ces modes de vraisemblance (générique, pragmatique, diégétique et empirique) charrie des valeurs, des représentations ou des procédés qui consolident le rôle du scénario, et de la projection d'usage, comme acte de langage performatif ; c'est-à-dire comme l'accomplissement simultané de l'articulation de signes reliés syntaxiquement (actes locutoires), de définition d'une situation d'énonciation et de sa pertinence (actes illocutoires) et surtout des effets provoqués ou attendus de la situation de communication (actes perlocutoires) au service de la progression de l'entreprise de recherche technologique.

## ***A - Le scénario, un acte de langage scientifique***

La compilation de signes et de symboles qu'est le scénario ne laisse planer aucun doute sur son genre littéraire d'appartenance : la littérature scientifique, et plus spécifiquement, le sous-genre que constituent les rapports d'activité ou livrables. Formellement, c'est un document de 39 pages dactylographiées et numérotées, ponctuées de textes et de schémas variés. Il est rédigé en anglais, *lingua scientificae* de la recherche contemporaine, dans un registre de langue soutenue avec un vocabulaire technique, sinon jargonneux.

La mise en page est sobre - seuls les tableaux et schémas sont égayés par de la couleur - et le document ne présente qu'une seule fonte typographique. Cette mise en page n'est pas le fruit du hasard mais répond au cahier des charges de l'ANR.

En termes d'organisation, le scénario reprend la structure classique d'un rapport d'activité scientifique. Le document est coiffé d'un en-tête qui en précise le titre (COPRIM Scenarios : Specifications) et l'identité du commanditaire (logo ANR). Il est parcouru d'un pied de page dans lequel est inséré un cartouche avec le nom du projet, la date, les auteurs du document, la version ainsi que le numéro de page. La structure du document (voir Figure 14) est rendue visible par l'adoption trois niveaux de titrage (ex : 2, 2.3, 2.3.1).

La page de couverture (voir Figure 15), d'une présentation sobre, est chargée de données renseignant sur :



- le nom du projet (COPRIM) ainsi que son nom de code (Projet ANR-07-TLCOM-04-COPRIM)
- l'objet du rapport (COPRIM Scenarios : Specifications)
- la date ainsi que la version du rapport (31.08.09, V3.0)
- la liste des auteurs du rapport identifiés par leur nom et leur institution de rattachement respective
- Un encadré rouge qui rappelle le caractère confidentiel du rapport ainsi que le détail de la liste de diffusion restreinte

La page de garde rappelle la liste d'autorisation de diffusion, la page suivante, l'historique du projet et une liste de mots-clés, puis vient une table des matières rappelant les sept parties du document (Glossaire, Introduction, Perception et régulation des frontières de la Privacy, Description des scénarios, Conclusion, Annexes et Bibliographie)

Figure 14.Extrait du sommaire

<b><u>Table of contents</u></b>	
<b>1</b>	<b>GLOSSARY ..... 6</b>
<b>2</b>	<b>INTRODUCTION..... 7</b>
2.1	SCENARIOS ANALYSIS' METHOD ..... 7
2.2	GLOBAL OVERVIEW..... 8
2.3	SCENARIOS GENERAL PRESENTATION..... 9
2.3.1	Payment..... 9
2.3.2	Transport ticketing..... 9
2.3.3	Smart poster (contactless token)..... 9
2.3.4	Device pairing (peer to peer)..... 9
<b>3</b>	<b>REGULATION AND PERCEPTION OF PRIVACY'S BORDERS..... 10</b>
<b>4</b>	<b>SCENARIOS DESCRIPTION..... 11</b>
4.1	PAYMENT..... 11
4.1.1	Detailed description..... 11
4.1.2	Analysis..... 17
4.2	TRANSPORT TICKETING..... 19
4.2.1	Detailed description..... 19
4.2.2	Analysis..... 26
4.3	SMART POSTER (CONTACTLESS TOKEN) ..... 27
4.3.1	Detailed description..... 27
4.3.2	Analysis..... 29
4.4	DEVICE PAIRING (PEER TO PEER)..... 31
4.4.1	Detailed description..... 31
4.4.2	Analysis..... 33
<b>5</b>	<b>CONCLUSION ..... 34</b>
5.1	ON THE SCENARIOS DESIGN AND DESCRIPTION ..... 34
5.2	ANALYSIS SUMMARIZING PART..... 34
<b>6</b>	<b>APPENDIX..... 36</b>
6.1	SOCIOLOGIC TOOLS..... 36
6.1.1	Beilot Gird..... 36
6.2	CRYPTOGRAPHIC PROTOCOLS AND ALGORITHMS ..... 36
6.2.1	SDA (Static Data Authentication) ..... 36
6.2.2	DDA (Dynamic Data Authentication) ..... 36
6.2.3	RSA (Rivest Shamir Adleman)..... 36
6.2.4	ECDSA (Elliptic Curve Digital Signature Algorithm)..... 37
6.2.5	DES (Data Encryption Standard) ..... 38
6.2.6	AES (Advanced Encryption Standard) ..... 38

Figure 15. Page de couverture du rapport

 	
<b>COPRIM Scenarios : Specifications</b>	
<b>Projet ANR-07-TLCOM-04 - COPRIM</b>	
<b>Date:</b> 31.08.09	<b>Issue:</b> V 3.0
<b>Authors:</b> <b>CEA LETI :</b> F. Marchand, G. Savry <b>UPMF:</b> B. Lenoir, B. Angerville, F. Forest <b>UVSQ :</b> L. Roulin, C. Delorme <b>INSIDE CONTACTLESS:</b> B. Fera, C. Malinval, Y. Harneault	

**CONFIDENTIAL**

**Restricted mailing list**

Mailing list	Name	Partner
ANR	Frank Tardif	
COPRIM Technical team	Benoit Fera	Inside Contactless
	Yves Harneault	Inside Contactless
	Oliver Lenoir	UPMF
	Emmanuel Angerville	UPMF
	Fabrice Forest	UPMF
	Lucie Roulin	UVSQ
	Oliver Savry	CEA-LETI
	Fabrice Marchand	CEA-LETI

The information contained in this document is the property of the contractors. It cannot be reproduced or transmitted to thirds without the authorization of the contractors.

1/39

Cette structure emprunte autant aux exigences didactiques du rapport d'activité que du formalisme de la démonstration scientifique. Le glossaire permet de neutraliser les éventuels contre-sens ainsi que d'user d'acronymes utiles aux démonstrations et au déchiffrement de celles-ci (voir Figure 16).

Figure 16. Extrait du glossaire

PIN	Personal Identification Number
RAM	Random Access Memory
RFA	Radio Frequency Analysis
ROM	Read Only Memory
RSA	Rabin Shamir Adleman public key cryptosystem
RSA CRT	RSA with the Chinese Remainder Theorem
SCA	Side Channel Analysis
SPA	Simple Power Analysis
URL	Uniform Resource Locator

L'introduction rappelle le cadre de la recherche ainsi que la problématique. La description des scénarios permet de limiter et de définir l'objet de recherche. Les analyses sont fondées sur la description préalable et forment une prémisse de développement. La conclusion clôt les réflexions entamées et ouvre sur les grandes lignes de travail postérieures. L'appendice permet de rendre compte d'outils et de références qui auraient pu parasiter le récit si elles avaient été placées dans le corps de la démonstration. La bibliographie renseigne sur les références utilisées en utilisant les normes de présentation d'usage.

En somme, la structure même du document ainsi qu'un certain nombre de signes et de symboles inscrivent celui-ci dans la tradition des rapports (livrables) scientifiques. Aucune exubérance ne permettrait au lecteur coutumier de littérature grise de s'y tromper : le document intègre un faisceau de conventions propres au genre scientifique. Ce faisant, le scénario observe scrupuleusement les règles de la vraisemblance *générique*, soit les règles permettant d'attribuer à un genre un type de récit.

## ***B - Le scénario, un acte de langage situé***

Le deuxième type de vraisemblance imbriquée dans le scénario est la vraisemblance *pragmatique* qui « renvoie quant à elle à la performance narrative, c'est-à-dire à la *crédibilité du narrateur et de la situation énonciative*. » (Mercier, 2009)

En effet, l'adhésion se fonde sur l'acte même de la narration, c'est-à-dire sur le caractère autorisé de celui qui s'exprime. Ainsi, le scénario est émaillé d'indices permettant d'assurer au lecteur une appréhension adéquate de la situation d'énonciation. Les coordonnées de celles-ci sont limpides : le document ne laisse planer aucun doute pour savoir d'où les narrateurs parlent et pour qui ils le font.

Tout d'abord, le document est émaillé de signes permettant d'identifier et de crédibiliser l'énonciateur. Le logo du projet COPRIM figure en page de couverture tout comme celui de l'ANR, qui est repris sur chaque page du document. Chaque auteur est rattaché à une institution partenaire, reconnue au sein de sa communauté scientifique respective. Ainsi, le narrateur est crédible, parce que, comme nous l'avons déjà démontré, il observe les normes du genre littéraire scientifique. Il est également crédible en ce qu'il, au risque de la tautologie, fait partie d'un projet financé par l'ANR, et enfin parce que le caractère restreint de la liste de diffusion atteste, au mieux de la crédibilité de ce qui est dit, *a minima* du caractère confidentiel des informations. La note de bas de page qui figure sur la page de couverture renforce cette crédibilité<sup>204</sup>.

Par ailleurs, le descriptif des différentes phases d'évolution du scénario (voir Figure 17), de sa création et sa relecture finale, donne à voir la somme de travail effectuée ainsi que l'intensité des échanges entre parties : l'effectivité de la collaboration entre les différentes parties au projet est ainsi affichée, à défaut d'être démontrée.

---

<sup>204</sup> «The information contained in this document is the property of the contractors. It cannot be reproduced or transmitted to thirds without the authorization of the contractors.»

Figure 17. Historique de la création du scénario

<u>Historical</u>		
Change record	Date	Issue
creation	01.02.09	v 1.0
scenario 1 description		v 1.1 to v 1.5
session opening added	16.03.09	v 1.6
skimming / relay attacks division	23.03.09	v 1.7
new framework adopted (cf. COPIL #4)	29.04.09	v 2.0
scenarios 2, 3 and 4 completed	05.06.09	v 2.1
sociological analysis integrated	10.08.09	v 2.2
conclusion update	21.08.09	v 2.3
Final review	31.08.09	v 3.0

En somme, et pour reprendre la terminologie de la linguistique, les actants et les circonstants sont mis en scène de sorte que le lecteur ne puisse pas douter de la légitimité de l'énonciateur. Celui-ci est un consortium dont la production offre de nombreux gages quant à sa légitimité à s'exprimer. Ce balisage du cadre de la communication renvoie à la notion de contrat de lecture entre un auteur et ses publics : avant même l'appréciation approfondie du contenu, l'objet de médiation entre l'auteur et ses publics affiche des garanties qui excluent à l'un comme aux autres d'être trompés par « la qualité de la marchandise ».

### ***C - Le scénario, un acte de langage prévisible***

Après avoir abordé la manière dont l'empaquetage du scénario contribue à consolider la vraisemblance de celui-ci, nous allons désormais nous pencher sur le contenu produit. L'une des caractéristiques de la fiction est qu'elle développe un mécanisme de vraisemblance fondé sur la cohérence de sa construction. C'est ce que Mercier nomme la vraisemblance *diégétique* : elle « renvoie à la cohérence de la mise en intrigue sur laquelle insiste particulièrement Aristote et que Pernot désigne par l'expression *vraisemblance interne puisqu'elle tient à la « prévisibilité logique du récit.* » (Mercier, 2009)



On a déjà vu que la structure même du récit, du fait de l'appartenance au genre scientifique et au sous-genre des rapports de recherche, portait en elle-même une forme de prévisibilité. Il en est de même pour la définition de la situation d'énonciation qui permet au lecteur d'anticiper le type de récit auquel il va être confronté et donc, son déroulement. Dans notre cas, il s'agit de démontrer que les différentes trames narratives qui traversent le scénario sont construites de telle sorte que leur déroulement peut être anticipé. Pour ce faire, il nous faut analyser le corpus en distinguant deux types d'énoncés constitutifs du scénario : ceux qui commentent le monde, ancrés dans la situation d'énonciation, et ceux qui le racontent, situés hors de la situation d'énonciation (Weinrich, 1973). Les premiers forment un discours sur la fiction visant à encadrer la réception du récit formée par les seconds.

### **1) La fiction commentée**

Ces énoncés comportent des indices renseignant sur la situation d'énonciation : l'équipe projet et l'environnement dans lequel se déroule le projet peuvent transparaître à la lecture de ces énoncés. Ceux-ci sont présents en trois endroits du rapport : l'introduction, la conclusion et les analyses relatives à chaque scénario<sup>205</sup>. Dans chacune de ces parties, on retrouve une forte présence des marqueurs d'énonciation ainsi qu'un enchaînement prévisible des événements du discours.

#### **Les marqueurs d'énonciation**

Concernant les marqueurs d'énonciations, quatre types peuvent être distingués : les circonstanciels de temps et ceux de lieu et les circonstanciels marqueurs de la présence de l'énonciateur et ceux du destinataire. D'abord, on repère l'omniprésence des circonstanciels de lieux dans le paratexte qui accompagne le récit. Le logo de l'ANR, les précisions sur la date d'émission du rapport, sur l'identité de ses auteurs ainsi que sur les intitulés du projet et des documents sont autant d'indices incontournables qui ancrent l'énoncé dans une situation sans équivoque. Ils participent à ne pas perdre de vue l'endroit d'où parle l'énonciateur : l'espace français de la recherche et développement subventionnée.

En ce qui concerne le temps de l'énonciation, celui-ci s'inscrit dans la temporalité discursive particulière qu'est le temps du projet, et plus précisément le temps de la projection d'usage. Les textes sont ainsi parcourus de marqueurs éloquents tels que :

- « *The first step of the analysis* »
- « *Directly related the previous step, we then draw* »

---

<sup>205</sup> Il s'agit des parties Analysis : 4.1.2 ; 4.2.2 ; 4.3.2 et 4.4.2

- « *In a third exploratory part, we extrapolate* »
- ou encore « *After having reviewed [...], we have found* » « *Bluetooth is assumed here to be the unique solution* ».

L'énonciateur relate un fait pour lequel il a une implication et une participation fortes. L'action est située dans un présent du « je-ici-maintenant » caractéristique du discours.

La présence de l'énonciateur est marquée par l'usage des prénoms personnels et des possessifs (« *we* » et « *our* » inclusifs de l'équipe projet : « *Drawing from our analyses, we will be able to establish a system of hypotheses that will help evaluate what poses a threat to privacy protection. Doing this, we will evenly assess the dual concepts of confidence/trust which are pivotal in this project. Our main objective is then to give insights to the role of design in privacy management* », « *We try to assess the use cases according to the amplitude of the technical available options' impact on privacy management.* », « *Trust is here involved only if we consider the validation function to be...functional* ».

C'est en partie en creux de la présence de l'énonciateur qu'apparaît le destinataire. En effet, celui-ci peut être considéré comme un prolongement plus ou moins étendu de l'équipe projet. Le « *we* » et le « *our* » peuvent ainsi inclure l'ANR mais pourraient aussi être entendus comme la voie de représentants de la communauté scientifique. Par ailleurs, le texte est jalonné d'instructions de lecture qui s'adressent aux destinataires telles que :

- « *Scenarios are then to be built and read by getting into the final users' shoes.* »
- « *If the presented use cases were exploited to help specifying the CPM, their writings will need a greater attention when they would serve as visual/textual aids during the acceptability tests.* »
- ou bien encore « *Furthermore, the following analysis should not be understood as a prediction of the use.* »

### **La logique du discours scientifique**

Les logiques des discours d'introduction et de conclusion tirent leurs caractères prévisibles du fait qu'ils empruntent au discours de la méthode scientifique. Ils sont fondés sur une logique de la démonstration scientifique : après un rappel du contexte de l'étude, l'objet de la recherche est défini et problématisé, un protocole d'étude est énoncé, justifié et mis en place, les résultats sont analysés et des conclusions sont tirées. Le plan et le déroulé du rapport respectent l'orthodoxie de la démarche scientifique.

Ainsi, l'introduction fixe le contexte et les objectifs de l'étude. Le déroulé de l'introduction se fait en trois temps :

- La partie 2.1 (« *Scenarios analysis' method* ») fait office de rappel du contexte et des objectifs de l'étude<sup>206</sup>. Dans cette partie est également introduit l'outil qui va servir d'élément central de l'analyse des résultats de l'étude. Cet outil (Voir Figure 18) qui vise à optimiser le rôle de protecteur de la Privacy du CPM, est révélateur de la croyance des concepteurs dans leur capacité à gérer en amont les problématiques liées perception de la Privacy. Ainsi, chaque moment-clé du scénario (voir D) correspond à une situation d'usage (« Use case »). L'accomplissement de chaque situation peut s'effectuer par le biais de différentes procédures de communication technologique. Chaque procédure abordée par l'équipe projet correspond à une option technique (« *technical option* ») susceptible d'être intégrée dans le dispositif CPM. Pour aider à l'arbitrage entre chacune des options, une grille d'analyse a été élaborée afin d'évaluer le rapport absolu et relatif de chaque option à la notion de Privacy. Trois dimensions ont été prises en compte. D'une part, un axe vertical permettant d'évaluer le degré de contrôle qu'aurait l'utilisateur sur le dispositif technologique. D'autre part, a été construit un axe horizontal donnant la mesure des retours informationnels offerts à l'utilisateur (« *feedback* »). Le croisement de ces deux axes produit quatre quadrants correspondant à une « *configuration d'usage* » particulière. Un troisième axe diagonal complète la grille d'analyse. Il oppose deux pôles fondés sur l'analyse de la confiance de Luhmann<sup>207</sup> : la confiance assurée (« *Confidence* ») et la confiance décidée (« *Trust* »).

---

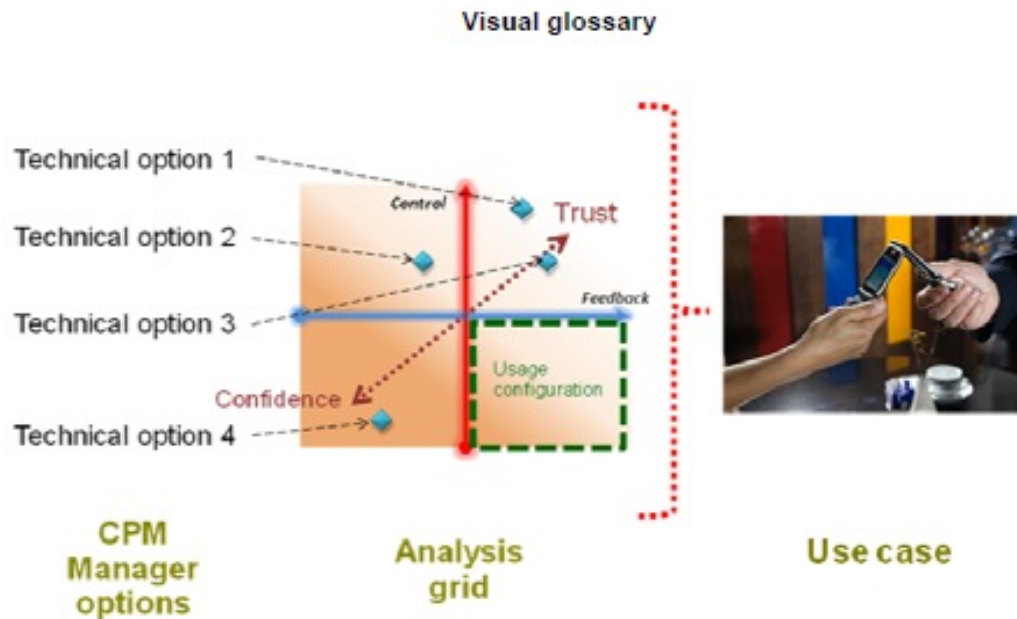
<sup>206</sup> “Our main objective is then to give insights to the role of design in privacy management : the available technical alternatives for each use case are not only distinguishable according to the control/feedback given to the user, they also endorse different philosophy of privacy management.”

<sup>207</sup> Nous reproduisons ici la note de bas de page présente dans le rapport et explicative de la différence entre ces deux types de confiance.

« Confidence's definition : « La confiance assurée, de même que la connaissance qui lui est nécessaire, se basent sur plusieurs éléments. Elle peut se fonder sur la capacité d'imposer des sanctions et sur le fait de savoir que le partenaire d'interaction sait aussi quelle sanction lui sera infligée s'il ne respecte pas les termes d'un accord. Les sanctions peuvent être formelles ou informelles, elles peuvent être étayées sur un réseau complexe d'obligations de parenté ou sur les dispositions de la loi concernant les contrats. Elles peuvent être immédiates ou intergénérationnelles, symboliques ou matérielles. » (our emphasis).

· Trust's definition : « Elle est ce dont nous avons besoin quand nous n'avons pas, ou ne pouvons pas avoir, une confiance assurée, en particulier quand nous ne pouvons pas prédire les comportements et leurs conséquences. La confiance décidée est ce dont nous avons besoin lorsque nous sommes en interaction avec des étrangers. Elle est ce qui est nécessaire quand nous ne pouvons pas connaître l'autre, i.e. quand nous ne sommes pas en mesure de lui attribuer un comportement ou de le prédire, parce que soit a) il n'existe aucun système au sein duquel des sanctions pourraient être imposées, soit b) on ne trouve aucun élément de familiarité ou de similitude permettant une telle attribution ou une telle prédiction. » (our emphasis). (See State of the Art for more details) »

Figure 18. Glossaire visuel



- La partie 2.2 (« *Global overview* ») prolonge la problématique esquissée en précisant l'arrière-plan politique de l'analyse et de ces conséquences. Les décisions découlant de l'analyse oscillent entre une conception centrée-utilisateur revendiquant donner la part belle de l'initiative d'usage à l'utilisateur et l'« *ubiquitous computing* » favorisant l'autorégulation des interactions par les objets connectés.
- La partie 3 (« *Regulation and perception of privacy's borders* ») est détachée du chapitre introductif dans le plan du rapport. Elle fait office de retour réflexif sur le travail engagé et permet aux auteurs d'en circonscrire la portée et de poser les limites du protocole adopté.

Les analyses liées à chaque situation d'usage consistent à passer chaque option technique (en ligne) au crible de trois variables (voir Figure 19) : les entités à qui incombe la responsabilité de la sécurité des échanges, le type de confiance qui en résulte et la désignation des responsables de l'échec de la sécurité<sup>208</sup>. Quelle que soit la situation envisagée, l'analyse emprunte toujours le même cheminement logique : le choix d'une option technique est à l'origine d'un enchaînement causal aboutissant à une situation d'équilibre ou de menace sur l'utilisateur/sur les organisations impliquées. Quelle que soit la

<sup>208</sup> Voir Chapitre IX.

situation d'usage, l'analyse aboutit systématiquement à l'interrogation du rôle dévolu à l'utilisateur, question résumée dans cet extrait lié à l'analyse de la séquence « smart poster » : « *The question is therefore : what kind of skills are we expecting the user to develop to manage a risk proof and privacy-enhanced communication?* ».

Figure 19. Analyse d'une situation d'usage (smart poster)

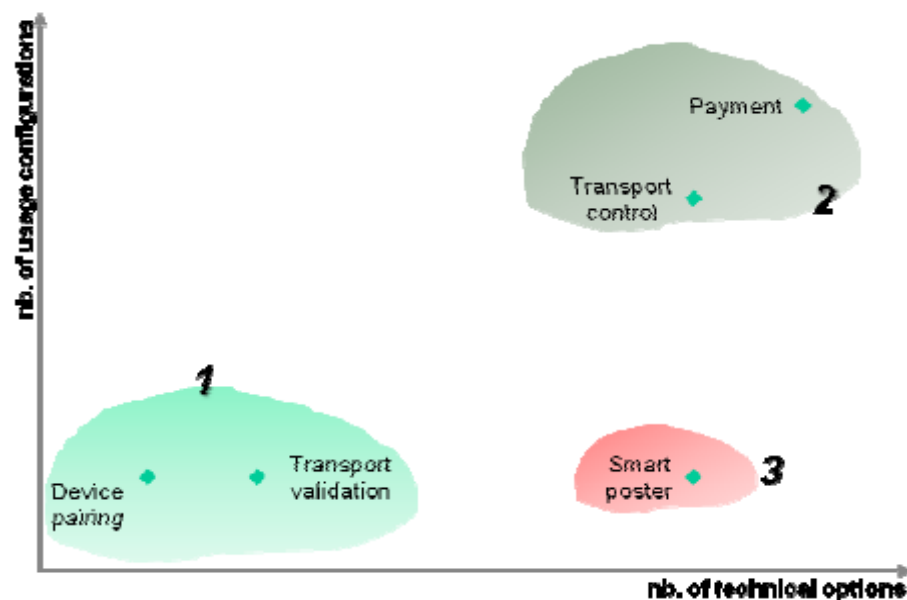
	Delegation of responsibility for security	Prevailing type of Confidence	Protection failure offloading process
Basic solution	<u>technology, individual, organization</u> <ul style="list-style-type: none"> <li>- mobile industry (phone builders/ service providers)</li> <li>- the individual (memory et dissimulating)</li> <li>- Transport company : machine and employees</li> </ul>	Trust	The user considers himself/herself as a possible liability in the system security breakdown.
Certif	<u>technology, individual, organization</u> <ul style="list-style-type: none"> <li>- mobile industry (phone builders/ service providers)</li> <li>- the individual (memory et dissimulating)</li> <li>- Transport company : machine and employees</li> <li>- Certifying organization</li> </ul>		The user considers himself/herself as a possible liability in the system security breakdown.
User + Certif	<u>technology, individual, organization</u> <ul style="list-style-type: none"> <li>- mobile industry (phone builders/ service providers)</li> <li>- the individual (memory et dissimulating)</li> <li>- Transport company : machine and employees</li> <li>- Certifying organization</li> </ul>		The user considers himself/herself as a possible liability in the system security breakdown. In that case, his/her involvement is more important than in the two previous others.

Enfin, en ce qui concerne la conclusion, elle consiste, d'une part, en un résumé de l'analyse, d'autre part, en une annonce des travaux à engager dans la suite du projet :

- La première partie de la conclusion (« *On the scenarios design and description* ») contient un ensemble de remarques et de réserves sur la portée du travail présenté. « *These propositions do not aim at being exhaustive but cover a wide range of possibilities in terms of security, privacy and control given to the user.* »

- La deuxième partie offre un résumé de l'ensemble des travaux présentés. Les différentes situations d'usage sont regroupées dans un graphique (voir Figure 20) qui croise le nombre de configurations d'usages et le nombre d'options techniques offertes. Trois groupes sont ainsi constitués et évalués en fonction de leur capacité respective à offrir ou retirer à l'utilisateur une plus ou moins grande latitude sur le « *contrôle/feedback/confiance/trust* » offert.

Figure 20. Grille d'analyse de la conclusion



## 2) La fiction racontée

La fiction racontée qu'est le récit fait également partie de la démonstration scientifique. Cependant, elle se situe dans l'univers du discours rapporté, d'un réel hors temps coupé de la situation d'énonciation. Ce sont ces éléments fictionnels. On en retrouve Bien que les énoncés présents dans la majeure partie de l'introduction soient intégrés à la situation d'énonciation<sup>209</sup>, des traces fictionnelles sont enclavées dans l'introduction sous l'intitulé « *Scenarios general presentation* » (voir Figure 21). Il s'agit d'un récit découpé en quatre phases : il s'agit de l'histoire d'une femme, Julie, qui grâce à son téléphone NFC, va pouvoir acheter des tickets de bus (« *Payment* »), valider et présenter ses titres de transport (« *transport ticketing* »), télécharger l'adresse internet d'un concert figurant sur une affiche

<sup>209</sup> Pour la partie 2.3, voir le point 2.

(« smart poster ») et se faire offrir une place de concert par échange de données (« peer to peer »). Chaque phase du scénario correspond à une activité associée au téléphone NFC.

*Figure 21. Scenarios general presentation*

### **2.3 Scenarios general presentation**

Four main scenarios have been set up to drive the works in the COPRIM project. They will be detailed in the next chapters.

#### **2.3.1 Payment**

Every morning, Julie takes the bus to go to work. Thus, she needs to buy bus tickets. She could buy paper tickets but she prefers not to charge her wallet and to use her telephone NFC. Indeed, her NFC phone contains an application of classic banking payment and an application of transport which manages the electronic ticketing.

#### **2.3.2 Transport ticketing**

Julie gets in the bus and validates the electronic ticket she has just bought. Other people have annual subscription held in their phone NFC transport application. During the run passengers tickets are checked by the company control staff.

#### **2.3.3 Smart poster (contactless token)**

Today, Julie takes the bus with Yves, her grandfather. During the run, Julie points out an e-poster about a concert she's interested in. Yves suggests buying her a seat with his own NFC phone, she accepts.

#### **2.3.4 Device pairing (peer to peer)**

Yves uploads the e-ticket he has just bought from his NFC phone to Julie's one. The Bluetooth file exchange is preceded by a NFC Bluetooth pairing.

Hormis certaines incohérences concernant la logique du récit, celui-ci présente une succession de faits dont la logique est incontestablement vraisemblable : emprunter un moyen de transport collectif grâce à un titre de transport préalablement acheté, se soumettre au dispositif de contrôle de la validité des titres de transport de la compagnie, être alerté durant ce temps de transport par une information publicitaire sur un loisir et se faire offrir une place de concert par un proche accompagnant n'a rien d'un récit loufoque, invraisemblable ou irréel. C'est même une histoire relativement ennuyeuse et fortement banale. En revanche, l'originalité de ce récit provient de son découpage en quatre phases distinctes : les situations d'usage. En effet, la logique de découpe de ces quatre séquences est liée au fait qu'à chacune d'entre elle correspond un type d'usage du NFC.

En réalité, le récit est donc déjà organisé pour favoriser le choix d'une échelle d'analyse par le groupe projet : autant le découpage en quatre séquences que l'abondance d'interactions

homme/machine constituent des facilitateurs de transport du récit à l'échelle atomique, une échelle plus manipulable en raison de son habilité à réduire les facteurs causaux. Ainsi à l'instar des livres-jeux, plus connus sous le nom de « livres dont vous êtes le héros », le groupe projet a constitué chaque situation d'usage comme un terreau fertile à l'émergence d'options techniques vraisemblables et d'analyses plausibles.

Ainsi, le récit élaboré par le groupe projet peut se lire selon deux niveaux complémentaires. Il y a, bien sûr, ce récit ennuyeux, sans relief, mais profondément vraisemblable (voir Figure 21). Il y a aussi cet entrelacement de procédures complexes parmi lesquelles il va falloir opérer des choix pour construire le chemin le plus protecteur de la Privacy de l'utilisateur. Le choix définitif d'une option technique, éclairé par l'analyse, sera ainsi celui d'un groupe-projet, héros d'une histoire qu'il écrit lui-même. Cette deuxième lecture connaît une traduction formelle liée à la première, mais plus étoffée et formellement différente. Elle correspond à la partie 4 du rapport : « *Scenario description* ».

Prenons l'exemple de la transmission d'information d'un objet (poster) à l'autre (téléphone), soit la quatrième séquence du récit, nommée « *smart poster* ». Le niveau de détail de l'interaction augmente tandis que le « bruit » de son environnement spatial, social, temporel, etc. disparaît totalement (voir Figure 22).

Figure 22. Description détaillée de la séquence *smart poster*

### 4.3 Smart poster (contactless token)

#### 4.3.1 Detailed description

The Smart Poster contains an URL in a tag. Once an NFC phone is passed in front of the poster with NFC activated, the NFC chip (in reader mode) reads this URL and sends it to the baseband processor. Then, Julie can obtain some information about the concert on the web for example or Yves can buy a ticket.

The protocol used for communication between the NFC and the reader is ISO/IEC 14443 Type B. It corresponds to the NFC Type 4 among the protocols defined by the NFC forum.

Une adresse URL, utilisée pour identifier les pages web, est encapsulée dans une puce intégrée au poster. Il suffit à Julie d'activer la fonction NFC de son téléphone et de le passer devant le poster pour avoir un accès direct à cette adresse URL et donc aux informations relatives au concert. Même à l'échelle atomique, l'enchaînement est logique, implacable, avec des menaces et solutions vraisemblables puisque puisées dans l'état de l'art scientifique par les partenaires du projet.



Trois options techniques sont proposées et leur description est alors limitée aux protocoles d'interactions entre objet. Dans l'option technique n°1 « *Basic Solution* », l'URL est simplement lue par le téléphone NFC (voir Figure 23). Pour l'option technique n°2 « *Solution with certification of the tag* », la puce intégrée au poster est certifiée par une autorité habilitée. Le téléphone NFC va vérifier ce certificat avant de télécharger l'URL (Voir Figure 24). Dans le cas de l'option technique n°3 « *Solution with certification and consistency control by the user* », il s'agit d'une modification à la marge de l'option n°2 avec l'adjonction d'une étape supplémentaire : l'utilisateur vérifie que les informations qui s'affichent sur son mobile sont bien celles auxquelles il s'attendait, et valide ensuite, le cas échéant, l'accès à la page Web (voir Figure 25).

Figure 23. Option technique n°1

#### 4.3.1.1 Basic solution

The URL is simply read by the NFC phone and sent to the baseband processor.

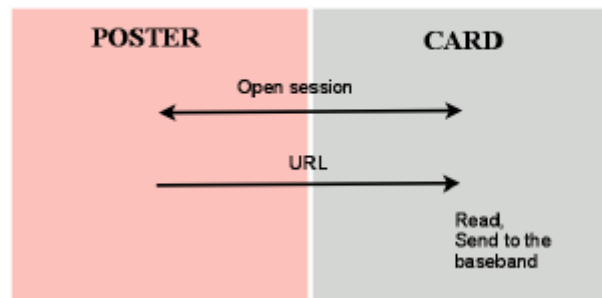


Figure 24. Option technique n°2

#### 4.3.1.2 Solution with certification of the tag

Each tag (on a poster) is certified by a known authority. The NFC chip verifies the certificate, and authorize (or not) the next step. If necessary, part of that verification (check for revocation lists for example) could be achieved over the air (OTA) – i.e. using 3G communication.

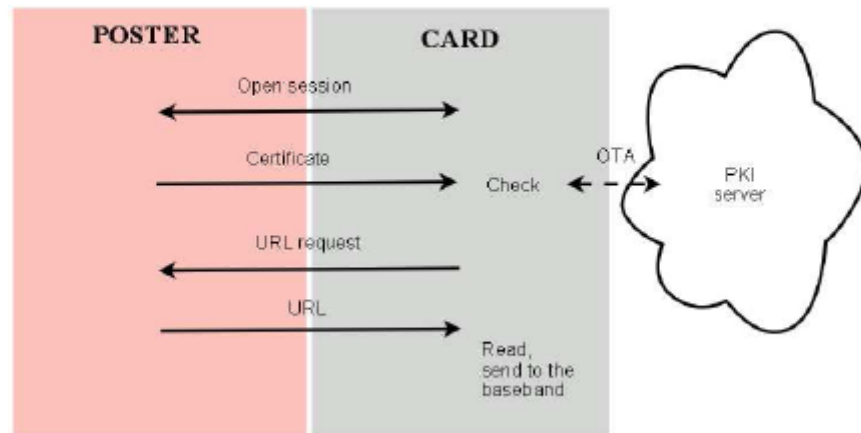
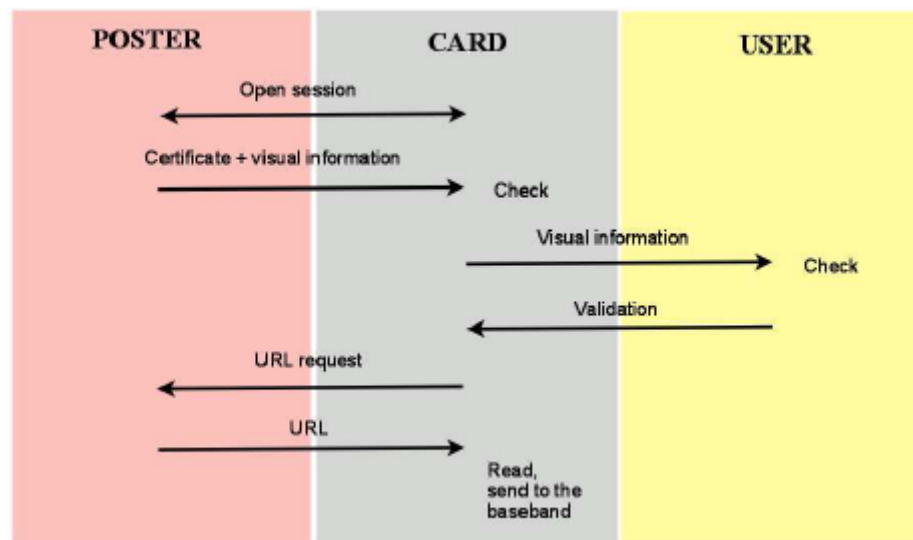


Figure 25. Option technique n°3



Ainsi, dire que le récit, la fiction racontée, précède le discours, la fiction commentée, tient de l'évidence. Autrement, la quête de vraisemblance serait avortée avant même son commencement. Néanmoins, ce que le scénario a de particulier tient du fait que le récit est un matériau généré dans l'optique de produire un discours efficace, c'est-à-dire actionnable pour la poursuite de l'activité du groupe projet. Cette opération, pour consciente et

volontaire qu'elle soit, est rendue d'autant plus aisée que producteurs et commentateurs du récit sont les mêmes personnes. Dès lors, le caractère vraisemblable du scénario, qu'elles que soient les formes littéraires revêtues et leur interrelation, s'en trouve à nouveau renforcé.

### ***D - Le scénario, un acte de langage social***

*« Everyday life is expanding to fill the spaces offered by the digitalization of ICTs. Reciprocally, ICTs are expanding their functionality and range to fill spaces of everyday life. »*

Ce constat du regretté sociologue des medias et des nouvelles technologies Roger Silverstone (Osimo, 2005 p. 103) est l'aboutissement d'une analyse de l'évolution de l'usage des TIC dans les sociétés occidentales contemporaines. Trois facteurs y concourent :

- La diminution de la taille des dispositifs techniques portatifs couplée à l'augmentation de leurs capacité de stockage, leur capacité à offrir des services convergents (téléphonie, internet, mail, radio, télévision, musique, etc.) est une invitation à la mobilité.
- Le changement du coût d'entrée pour accéder à ses TICs
- Le troisième facteur est la création de réseaux à la fois immédiats, personnels, locaux, et étendus et globaux.

Nous avons déjà insisté sur le fait que la prévisibilité du récit contribuait à le rendre plus vraisemblable. Ici, nous souhaitons démontrer que la vraisemblance du récit se construit également sur la capacité de celui-ci à transcrire un état du monde et de ses relations. C'est ce que Mercier nomme la vraisemblance empirique qui *« concerne précisément cette conformité de l'univers représenté à l'expérience commune, expérience qui inclut tout autant des connaissances, des faits attestés, que des opinions ou des représentations et qu'on ne saurait donc réduire aux lois physiques et aux données historiques. S'y trouvent réunies l'empiriquement possible et les idéologies qui fondent la représentation du monde et des comportements. »* (Mercier, 2009)

Le scénario, et en particulier le récit, se construit comme le reflet d'un état de l'opinion, un miroir des représentations sociales. Nous allons voir qu'il regorge de références explicites à l'adhésion à une forme de déterminisme technique associant l'idée de progrès social à la diffusion de technologies adéquates.

## 1) Le récit du progrès

D'abord, le scénario verse dans l'idéologie du progrès scientifique en conférant à l'évolution technologique un caractère de nécessité, d'universalité et d'irréversibilité. Dans le paiement et la validation des titres de transport, le téléchargement et l'échange de données sur téléphone mobile, ce sont des besoins de déplacement, d'acquisition de biens matériels ou immatériels, de transmission intergénérationnelle qui sont satisfaits. Et au-delà de leurs satisfactions, qui auraient pu avoir lieu sans l'existence du téléphone NFC, c'est la facilitation offerte par la technologie qui est mise en avant. Le scénario inscrit le téléphone NFC, ainsi que les usages qui y sont associé, dans une dynamique qui associe la dissémination de l'usage des technologies portatives au progrès. Un imaginaire collectif du progrès, nécessairement scientifique ou technique, qui est invariablement caractérisé par sa capacité à prendre pouvoir sur les contraintes (Scardigli, 1989). Dans le scénario, rien n'est impossible mais tout est nécessaire. Le doute plane uniquement sur la meilleure option à choisir pour garantir la Privacy des utilisateurs.

Il en est de même pour le discours qui porte sur l'analyse des scénarios. L'établissement d'un lien de causalité entre configuration socio-technique et attribution de responsabilité suppose l'existence d'une économie de la responsabilité : dans un marché dans lequel l'offre crée la demande (techno-push), l'existence de mécanismes d'assurances pour combler les éventuels dysfonctionnement de ce marché repose sur une distribution préalable des responsabilités échues à chacun des acteurs. Ainsi, les menaces qui pèsent sur la Privacy et/ou la sécurité touchent, bien entendu l'utilisateur potentiel – c'est la raison d'être du projet, mais elles constituent aussi une menace pour l'ensemble des acteurs de ce marché en devenir. Le CPM est ainsi intégré dans l'arsenal de technologies disponibles aux acteurs pour se prémunir au mieux de la survenance d'attaques ou de dysfonctionnement. En creux, se dessine également dans le discours sur le scénario l'embryon d'une économie de soutien aux défaillances de ce marché, économie qui repose sur la distribution réelle ou perçue des responsabilités de chaque acteur, c'est-à-dire de leurs droits et devoirs. Ce faisant, le scénario prévoit l'existence de technologies d'assurances garantissant à ce nouveau système une forme de pérennité conservatrice et innovante. Pérenne, car le système repose sur l'existence de palliatifs et d'assurance à ses propres défaillances. Conservatrice, car les nouveaux usages s'inscrivent dans un pattern de pratiques sociales éprouvées et familières. Innovante, car l'introduction de la technologie NFC suppose l'anticipation de la création d'un éco-système inédit. Le récit du progrès est empreint d'un enthousiasme fonctionnaliste reposant sur une mécanique du succès qui laisse peu de place à l'invraisemblable.

## 2) Objet magique

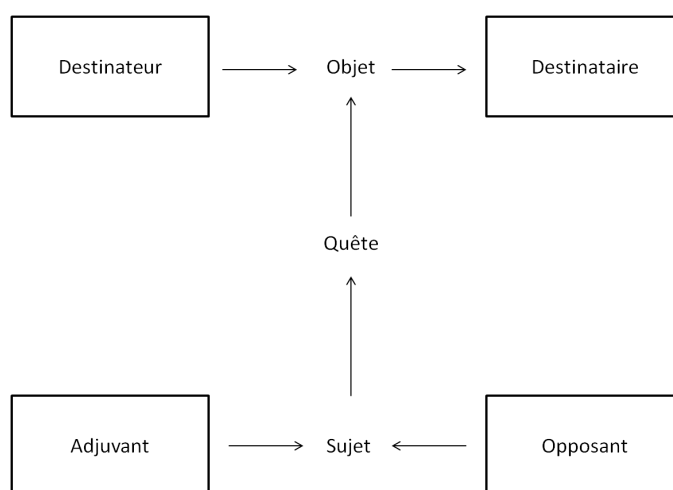
Etrangement, l'envers du décor rationaliste et positiviste, est un univers magique et fantasmagorique. Le progrès s'envisage comme « *un rite magique dans la célébration duquel nous sommes tous réunis. Ce retour en force du surnaturel vient ironiquement interpeller notre époque, éprise de rationalité.* » (Scardigli, 1989 p. 110)

La technologie et son usage sont imprégnés d'un « *animisme magique* » (Beaune, 1980) qui fait écho à l'objet magique primitif de Simondon et qui inscrit celle-ci au centre d'un schéma narratif dont elle est l'adjuvant magique qui débloque la situation du héros de l'intrigue.

En effet, le recours au schéma actanciel de Greimas (1966) comme outil d'analyse de chacune des phases du scénario renseigne sur le maintien de la portée magique de l'objet quelle que soit la séquence abordée. Dans ce schéma d'inspiration structuraliste (voir Figure 26), la narration du récit est invariablement résumable par les relations entretenues entre un nombre d'actants<sup>210</sup> réductibles à :

- Un destinataire dont le rôle est de commanditer une quête au profit d'un destinataire.
- Un sujet dont l'objectif est la réalisation de la quête commanditée à travers la conquête d'un objet.
- Des adjuvants et des opposants qui respectivement favorisent l'accomplissement de la quête ou contribuent à son irréalisation.

Figure 26. Schéma actanciel



<sup>210</sup> Notons qu'un actant peut être constitué de plusieurs personnages et que plusieurs actants peuvent être réunis en un personnage unique.

L'application de cette grille de lecture à notre cas d'espèce ( voir Figure 27 et Figure 28) met en lumière le fait que le téléphone NFC soit toujours placé comme l'adjuvant magique d'une quête dont les opposants se lisent toujours dans un rapport de temporalité comparative : est opposant la contrainte que le téléphone NFC parvient à atténuer ou abolir ; l'existence de la contrainte est donc consubstantielle de l'agissement du téléphone NFC. La société devient à la fois l'émetteur et le récepteur de la quête, par la médiation technologique et l'action d'un héros universel ou interchangeable.

*Figure 27. Schéma actanciel détaillé du scénario par séquence.*

	Payment	Transport ticketing	Smart poster	Device Pairing
<b>Actants</b>				
Emetteurs	Les services bancaires, les services de transport	Les services de transport, les assureurs des agences de transports, les organismes de subventions des usagers...	Les promoteurs du concert, les agences de publicité, les entreprises de mobiliers urbains...	L'organisme de vente de billets, le promoteur du concert, les services bancaires...
Destinataires	Le public	Les usagers/la sté de transport	Julie/Yves/ les usagers/ les clients potentiels du concert	Julie/ les usagers/le public du concert
Héros	Julie	Julie	Julie	Yves
Objet de la quête	L'achat de tickets de transport	validation du ticket de transport	L'achat de place de concert	Le don de place de concert
Adjuvant/ Objet magique	Le téléphone NFC permet à Julie d'avoir un paiement facilité	Le téléphone NFC permet une validation et un contrôle simplifié	Le téléphone NFC permet à Julie de recueillir des informations sur le concert et à Yves de procéder à un achat dématérialisé	Le téléphone NFC permet de donner des places de concert
Opposants	Le caractère laborieux de l'achat de ticket en format papier, le stockage et rangement de titres de transport papier	Les difficultés inhérentes au contrôle, la décentralisation des informations, le temps de contrôle	L'impossibilité de recueillir des informations complémentaires in situ et de procéder à un achat immédiat et simple	L'impossibilité de transmettre des données électroniques par un geste simple et intuitif

Figure 28. Schéma actancier simplifié du scénario par séquence.

	Payment	Transport ticketing	Smart poster	Device Pairing
<b>Actants</b>				
Emetteurs	La société			
Destinataires	La société			
Héros	Un ou plusieurs membres de la société			
Objet de la quête	Un besoin social			
Adjuvant/ Objet magique	Le téléphone NFC			
Opposants	Les pratiques du passé			

### 3) Appropriation

Abolir le temps, la distance, le coût et la difficulté des transports (de biens, de services, de personnes et d'informations) ancrent ces « télétechnologies » (De Gournay, 1997 ; Guillaume, 1997) dans les modalités nouvelles de la « *commutation* : toute opération, le plus souvent programmée et automatisée car fondée sur une classification, un regroupement, une structuration hiérarchique préalables, de recherche et de mise en relation d'éléments d'un ensemble quelconque (...). La fonction de commutation est présente dans tous les domaines de la communication (téléphonie – d'où ce terme est emprunté –, courrier postal, annuaires, index, dictionnaires, bases de données, hypertextes, ordinateurs...) mais pas seulement : la ville est, elle aussi, par excellence, un système de commutation puisqu'elle forme un système complexe de réseaux de transports, de télécommunications, de commerces, de rencontres, d'échanges ... ».

Cette co-présence des choses et des êtres renforce l'impression de facilité d'usage et d'appropriation qui se fonde dans l'immédiateté des rapports et la transcendance des échanges. L'objet téléphone NFC est considéré comme une triple prolongation : le geste, la perception sensorielle et la projection anthropologique ne fondent qu'un avec l'utilisateur qui, lui-même, est fondu dans le système de commutation. L'utilisation du présent comme

temps du récit reflète, au-delà de son utilité comme temps de description, l'incorporation du récit dans un *Zeitgeist* contemporain et donc vraisemblable. C'est exactement ce qui a pu être constaté, non pas dans l'étude d'autres fictions, mais dans une enquête sur le rapport à l'objet technique. L'usage répété du présent par les enquêtés ne tenait pas simplement d'une facilité de langage mais était révélateur du pouvoir qu'à le présent de simplifier, fédérer et dépouiller le récit de tout élément d'irréel ou d'invraisemblance :

*« Le présent peut se décrire comme un état de conscience lié à un moment donné; comme si l'on opérât une coupe transversale dans l'écheveau des multiples chronologies différentielles qui parcourent une civilisation. Cet état de conscience ne gomme pas les différences mais leur insuffle une cohésion qui les rend opérationnelles ici et maintenant et peut aller jusqu'à tendre des ponts aux une et aux autres. Ce rôle fédérateur, le présent le joue au niveau du situationnel, marge entre l'histoire individuelle qui sédimente conformités et distinctions, et le social qui englobe ces aspects dans une échelle plus large. Le situationnel précède l'individuel dans les données de l'environnement, en organisant des agencements particuliers qui sont autant de ponctuations socio-chronologiques. Le rapport au monde technique est donc rapport de transversalité, tant au niveau macro-sociologique, où l'état social est aussi à la croisée d'une multiplication des échelles de temps, qu'au niveau individuel où se jouent les combinatoires particulières qui localisent l'histoire en des formes et situations circonstanciées. Le présent est donc unificateur en ce qu'il regroupe dans une même conscience des états étrangers les uns aux autres. Mais encore, il estompe l'origine des objets, oublie leur parcours d'accès jusqu'à lui pour ne retenir d'eux que leur position dans l'espace. »* (Sansot, Chalas & Torgue, 1984 p. 6)

Scientifique, situé, prévisible et social, le scénario a été analysé comme cet ensemble d'actes de langages multidimensionnel qui :

- combine indistinctement des règles linguistiques établies – actes locutoires,
- produit un type d'informations définies – actes illocutoires,
- et produit l'intéressement des publics par leur caractère vraisemblable – actes perlocutoires.

En agissant dans le temps du projet, un temps de fiction, le scénario déporte l'enjeu de véridiction vers l'avenir de l'épreuve scientifique et de celle des faits. Nous allons constater, dans le chapitre suivant, que la vraisemblance conquise par la fiction s'appuie également sur un système de croyance partagée entre les publics et les auteurs car « *La vraisemblance*



*rappelle que la fiction, dans sa relation au lecteur, correspond non seulement à un acte de langage mais aussi à un acte de croyance provisoire. » (Mercier, 2009)*

## X - Le scénario : acte de croyance

---

Le scénario est un acte de croyance qui donne à voir une forme *d'enthousiasme technologique*. En effet, ses auteurs s'octroyent indistinctement une capacité de prédire, voire un don de divination, le droit à l'intuition couplé sans heurt à l'attachement au rationalisme technologique, et entendent la technologie de manière exogène, une force, si elle est maîtrisée, qui peut être une bénédiction pour la société. Etymologiquement, le mot enthousiasme signifie l'inspiration ou la possession par le divin. On retrouve ici une filiation avec les formes de pratiques de l'usage évoquées dans la première partie (poétique, pythique et sybilline). Détaché de toute connotation religieuse, cet enthousiasme se manifeste par le pouvoir explicatif donné à la technologie : elle se fait cause et conséquence de l'à-venir. Cet acte de croyance s'exprime par la contrainte de considérer comme vraisemblables :

- (1) l'avènement d'un système technique particulier
- (2) la soumission de l'*usage* à l'injonction d'innover technologiquement et
- (3) l'indétermination forte qui pèse sur la caractérisation de la technologie en développement.

Ce faisant, le scénario est un acte de croyance en une organisation du monde, une « *classification* » (Bowker & Star, 1999). C'est une « *segmentation spatiale, temporelle ou spatio-temporelle du monde érigée dans le but de mettre les choses en ordre afin de pouvoir travailler dessus* ». Selon Star et Bowker, une compréhension idéal-typique des classifications leur associe trois qualités :

- 1) elles sont consistantes en ce qu'elles répondent à des principes de classification unique
- 2) les catégories créées sont mutuellement exclusives
- 3) le système de classification est complet et fini.

En se saisissant du concept de « *classification* », nous souhaitons faire état de l'influence de *l'enthousiasme technologique* sur le travail de projection d'usage. Le concept permet d'aborder la question de cette forme exploratoire de coopération qui, *a priori*, échappe à toute forme de standardisation. En effet, Star et Bowker soulignent les rapports étroits qui unissent classifications et standards<sup>211</sup> : tandis que les standards sont nécessairement issus

---

<sup>211</sup> Pour les auteurs, les standards ont plusieurs dimensions listées ici exhaustivement par souci de clarté :

d'un travail antérieur de classification, les classifications peuvent ou non devenir standardisées. Pour Star et Bowker, à défaut de standardisation, les classifications ont pour caractéristiques d'être *ad hoc*, d'avoir une diffusion limitée à un individu ou à une communauté locale et/ou ont une durée de vie limitée. Ces classifications, qui s'expriment dans l'action, peuvent devenir des objets de collaboration entre des mondes sociaux différents. Ainsi, avant d'aborder de manière approfondie les formes de coopération à l'œuvre lors du travail de projection d'usage, nous avons voulu interroger *l'enthousiasme technologique* en tant qu'acte de classification et de coordination. Sans préjuger qu'il soit un « *objet-frontière* » à part entière, nous voulons cependant ici démontrer la manière dont cet enthousiasme a pesé sur la fabrication et la mise en accès de l'information produite dans le projet<sup>212</sup>. Aussi, nous souhaitons ici entamer la réflexion sur le caractère de ces classifications au sein d'un réseau local de conception. Nous le ferons en nous intéressant au mode de gestion par projet, au *problème* que le projet se propose de résoudre et aux figures de l'utilisateur qui le peuplent comme trois éléments révélateurs de la performativité de cette classification. Nous verrons ainsi que bien que la classification soit *ad hoc*, locale et limitée à la durée du projet, *l'enthousiasme technologique* qui en constitue le soubassement en étend l'ampleur. Sans constituer pour autant un standard, et parce qu'elle s'inscrit dans une logique projective, la classification franchit les frontières du projet en établissant des catégories dont la validité s'étend aux configurations socio-techniques dans lesquelles s'insère la projection d'usage. C'est là l'une des composantes du retour sur l'investissement de forme fictionnelle. C'est la classification d'un monde à venir qui dépasse le réseau local du projet, le réseau global à l'intérieur duquel il s'insère : elle est description parcellaire mais performative d'un projet de société.

---

« 1. A 'standard' is any set of agreed-upon rules for the production of (textual or material) objects.

2. A standard spans more than one community of practice (or site of activity). It has temporal reach as well, in that it persists over time.

3. Standards are deployed in making things work together over distance and heterogeneous metrics. For example, computer protocols for Internet communication involve a cascade of standards (cf. Abbate and Kahin, 1995) which need to work together well in order for the average user to gain seamless access to the web of information. There are standards for the components to link from your computer to the phone network, for coding and decoding binary streams as sound, for sending messages from one network to another, for attaching documents to messages, and so forth.

4. Legal bodies often enforce standards - be these professional organizations, manufacturers' organizations or the State. We might say tomorrow that volapük (a universal language that boasted some 23 journals in 1889 (Proust, 1989: 580)) or its successor Esperanto shall henceforth be the standard language for international diplomacy. Without a mechanism of enforcement, or a grassroots movement, we shall fail.

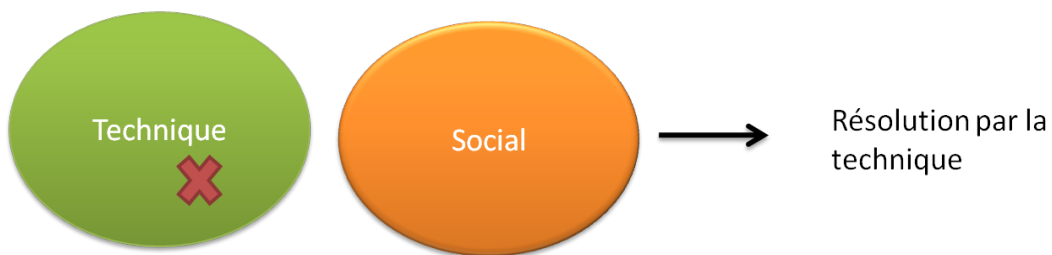
5. There is no natural law that the best standard shall win - QWERTY, Lotus 123, DOS and VHS are often cited in this context. The standards that do win may do so for a variety of other reasons: they build on an installed base, they had better marketing at the outset, and they were used by a community of gatekeepers who favored their use. Sometimes standards win due to an outright conspiracy, as in the case of the gas refrigerator documented by Cowan (1985).

6. Standards have significant inertia, and can be very difficult and expensive to change.» (Bowker & Star, 1999 p. 13-14)

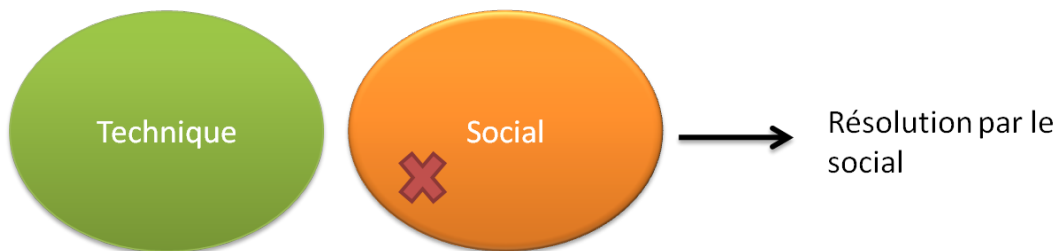
<sup>212</sup> « Formal classification systems are, in part, an attempt to regularize the movement of information from one context to another; to provide a means of access to information across time and space. » (Bowker & Star, 1999 p. 290)

Nous commencerons notre exposé en démontrant la manière dont le projet commande aux participants d'avoir foi dans l'avènement d'un macrosystème technique particulier, l'Intelligence Ambiante (1). De cette croyance obligée découle un système de classification du monde à venir qui débrouille les liens étroits entre le « technique » et le « social » : ce sont deux sphères en interaction mais dont les ressorts de fonctionnement sont internes et propres à chacune. Dès lors, la qualification d'un problème a de lourdes conséquences sur sa résolution. Trois cas de figures se présentent ainsi. Soit le problème est défini comme exclusivement « technique », ce qui implique que sa résolution le soit également (Figure 29).

*Figure 29. Résolution par la technique*



*Figure 30. Résolution par le social*



*Figure 31. Résolution mixte*

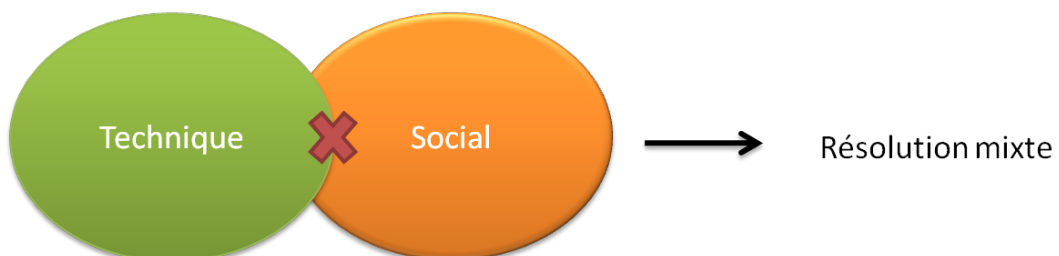
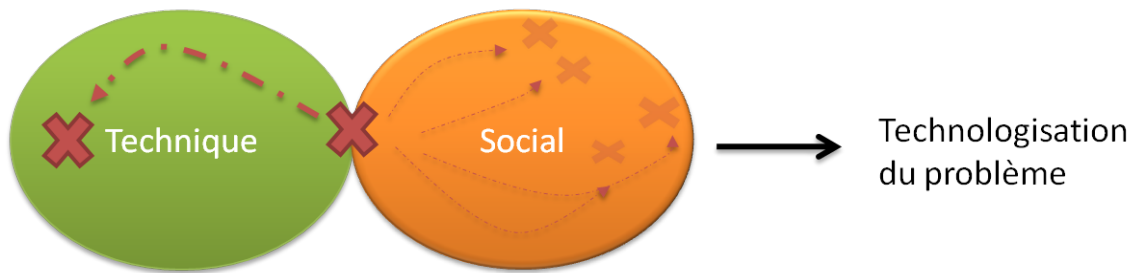


Figure 32. Technologisation du problème



Soit le problème est compris comme appartenant à la « sphère sociale », et alors les formes de solutions sont aussi « sociales » (Figure 30). Soit le problème est considéré comme impliquant du « technique » et du « social », et alors la forme de résolution recherchée sera mixte ou sociotechnique (Figure 31).

Cependant, nous verrons que la définition du problème se fait également en fonction de la perception de la disponibilité des moyens dont disposent ceux qui y sont exposés. Autrement dit, l'un des moyens de faire rentrer un problème dans le champ d'actions et de compétences que constitue le projet (réseau local) consiste à en modifier la nature des composantes ou alors d'en réduire certaines au silence. Si le projet est technologiquement enthousiaste, il incombera aux participants de *technologiser* un certain nombre d'éléments dont la nature « sociale » est dérangeante mais n'échappe pas complètement à son spectre. Les éléments résiduels seront considérés en filigrane, comme éléments existants mais périphériques à la sphère d'intervention du projet (

Figure 32).

Nous démontrerons donc que la mise en intrigue de l'*usage* s'effectue par un assujettissement du monde à la sphère technique. Non seulement, l'*enthousiasme technologique* impose de démêler le technique du social, mais il oblige certains éléments compris comme « sociaux » à trouver des formes d'expression technique afin de se donner les *moyens*<sup>213</sup> de rendre domesticable le monde. Nous illustrerons ce phénomène de *technologisation* en deux temps. Tout d'abord, en considérant la manière dont la

<sup>213</sup> Bruno Latour, dans un article intitulé «La fin des moyens» souligne le fait que l'essence immaîtrisable des techniques est rendue invisible par l'habitude d'usage d'une innovation : « La complication même des dispositifs, par l'accumulation des plissements et des détours, des couches et des retours, des compilations et des réarrangements, interdit à jamais la clarté de la raison droite sous le patronage de laquelle on avait d'abord introduit les techniques. Pourquoi donc certaines traditions occidentales dominantes parlent-elles malgré tout des techniques comme ce qui est susceptible de maîtrise ? Pourquoi ce qui devrait apparaître comme l'immaîtrisable se trouve-t-il toujours, en fin de compte, regroupé dans le règne de simples moyens ? » (Latour, 2000)

« sécurisation technique » de l'information échangée s'est imposée comme forme de résolution d'un problème impliquant sphères technique et sociale (2). Ensuite, nous nous attarderons sur une figure marquée comme faisant partie de la « sphère sociale » : l'utilisateur. Nous l'utiliserons pour illustrer le phénomène de *technologisation* d'un élément social. Nous montrerons que sa présence dans le projet est plurielle mais que cette pluralité d'être au monde rencontre une pluralité de traitements au sein du projet selon le degré de *technologisation* des figures abordées. Ainsi, nous soulignerons le fait que le projet contraint l'utilisateur à l'adoption d'une posture ergonomique d'utilisateur, posture qui offre des prises « techniques » aux parties au projet. En arrière-plan du projet, d'autres postures apparaissent comme des « *catégories résiduelles*<sup>214</sup> » placées hors de portée du faisceau de compétences du réseau local par le système de classification. Nous aborderons enfin les liens entre classification et modes de représentation de l'utilisateur dans le projet (3).

Aussi, le découpage analytique auquel nous avons procédé fait écho à la classification du monde par les acteurs du projet et pourrait laisser croire en l'adoption volontaire d'une posture déterministe de notre part. Les deux parties suivantes pourraient être lues comme une entreprise de négation du « *tissu sans couture* » (Hugues, 1986) au sein duquel « technique » et « social » s'emmêlent. Il serait, en effet, tentant de considérer l'utilisateur comme l'entrée choisie pour appréhender le « social » et la sécurité comme entrée pour le « technique ». En vérité, ce découpage analytique procède d'abord des pièges inévitables tendus par l'usage d'un langage de sens commun :

*« Of course, one could say that an author subscribing to the objectives of a seamless web approach should not be writing a sentence like this, using phrases such as “technical artifact” and “social impact”. I think that such pedantic criticism is unfruitful. The substantial methodological challenge is to develop analytical concepts that will allow us to realize the aim of analyzing technology and society in such a “seamless web way”, but on our way toward that goal one has to make do with what there is—using common language, but as carefully as possible. »* (Bijker, 1992 p. 102)

Sur un plan plus analytique, ce découpage s'explique également par notre volonté de comprendre les acteurs en saisissant leurs propres visions. En postulant donc que celles-ci puissent emprunter le découpage de sens commun qui distingue donc le « technique » du « social », nous avons souhaité explorer distinctement ces deux briques d'éléments de la

<sup>214</sup> « Classification systems always have other categories, to which actants (entities or people) who remain effectively invisible to the scheme are assigned. A detailed analysis of these others throws into relief the organizational structure of any scheme (Derrida 1998). Residual categories have their own texture that operates like the silences in a symphony to pattern the visible categories and their boundaries. » (Bowker & Star, 1999 p. 325)

projection d'usage sans pour autant méconnaître leur intrication, ce afin de mieux rendre compte du caractère dynamique du processus de *technologisation*.

## ***A - Le projet, réseau local relais de l'enthousiasme technologique***

L'exploration anthropologique du projet (comme objet de recherche) par Jean-Paul Boutinet (2007) va nous servir de base à la caractérisation de celui-ci comme structure relais de l'enthousiasme technologique.

Le projet COPRIM appartient à ce que Boutinet nomme les « *anticipations cognitives* » qui ont « *comme première préoccupation de percer le mystère du futur, en cherchant à connaître certains de ces aspects. Une telle connaissance a certainement comme fonction, entre autres, de conjurer tout ce dont ce futur est porteur [...]* » (p. 62), « *elles parlent d'abord de ce qui n'existe pas mais pourrait bien exister dans un avenir éloigné, en un lieu indécis.* » (p. 64) et « *[...] leur problème n'est pas d'imaginer n'importe quel futur plus ou moins distancié, futur objectif ou futur imaginaire. Il s'agit d'un futur personnel que l'auteur de l'anticipation va chercher à faire advenir.* » (p. 66)

En effet, le projet COPRIM se greffe sur le paradigme de l'Intelligence Ambiante dont l'avènement est considéré acquis comme l'attestent ces extraits de l'annexe technique au projet :

« *Le déploiement rapide des systèmes sans contact fait que ces derniers font d'ores et déjà partie des produits électroniques utilisés quotidiennement par des millions de personnes. On peut prendre comme exemple le domaine des transports publics. Ces dispositifs représentent une catégorie de composants numériques qui sont à la base de la future Intelligence Ambiante : cartes à puce et étiquettes RFID.* » (annexe technique 2008 p. 3)

« *With the trumpeted arrival of Ambient Intelligence (AmI), digital data Privacy is a key point. Several low resources smart devices have shown some connections with Privacy concerns:*

- *RFID electronic tags for items identification*
- *e-Citizen contactless cards (e-passport, e-identity, ...) for person identification*

*In that "Privacy situation", the main drawback of these contactless systems is that there is no switch on/switch off mechanism to assess the will of the owner to use them. They can be remotely and covertly activated and triggered without the awareness of the owner. Privacy is the ability of an individual or group to keep their lives and personal affairs out of*



*public view, or to control the flow of information about them. It is clear that AmI<sup>215</sup> may endanger the Privacy of citizens. On the other hand, AmI aims to offer a lot of on-line services that you can get only if you identify yourself or the items you are dealing with. So the difficult. » (annexe technique 2008 p. 10).*

Il est donc bien question ici de construction d'un futur, dans lequel le projet s'insère en cherchant à le modifier en considérant la sécurisation de certaines formes technologiques de communication comme problématiques pour la protection de la « *Privacy* ».

Cette description performative d'un monde à venir ne saurait être limitée à un processus de création *ex nihilo*. L'annexe technique au projet (annexe 4) offre une description du contexte du projet scindée en deux parties. Dans la première partie (« *Digital world and Privacy* »), l'ancrage dans le paradigme flou<sup>216</sup> de l'Intelligence Ambiante est affirmé et participe de la dimension créative du projet ; il ouvre notamment sur une liste exhaustive de fonctions auxquelles le dispositif devrait idéalement répondre et fixe les priorités sur lesquelles doit se concentrer le projet.

La deuxième partie, intitulée « *Contactless and Privacy research works* », contraste vivement avec la première, en ce qu'elle fait succinctement état de propositions de solutions émises par des laboratoires de recherche pour aborder le problème reconnu de la protection de la « *Privacy* ». Ainsi, en compilant des formes d'anticipation fondées sur l'intuition empirique et sur les dernières avancées scientifiques (voir première ligne du Tableau 6), le projet relève à la fois de la prévision et de la prévoyance dont la finalité est en réalité identique comme l'affirme Boutinet :

*« [...] Prévoyance et prévision [...] essaient chacune à sa manière, c'est-à-dire soit empiriquement, soit scientifiquement, d'anticiper des états possibles, les plus vraisemblables de l'avenir. » (Boutinet, p. 58)*

Le projet COPRIM répond donc à un « mode d'anticipation adaptatif » relevant à la fois de la conjecture et de la prédiction.

---

<sup>215</sup> AmI est l'acronyme anglais pour Ambient Intelligence.

<sup>216</sup> Dans un article publié dans le quotidien Le Monde daté du 24 avril 2009, titré « L'internet des objets n'est pas celui que vous croyez ! », Daniel Kaplan fustige la confusion régnant sur la définition de la notion d'Internet des Objets « censée traduire la mise en connexion généralisée des espaces et des choses ». D'abord, parce qu'elle désigne tour à tour le « RFID et sans contact » et fait référence à l'étiquetage électronique généralisé des objets, des lieux, voire des êtres, à des fins d'identification », tandis « D'autres y ajoutent les capteurs, des objets producteurs de données. » et que « le plus souvent, dans la littérature, les discours et les stratégies, on omet d'y ajouter les « actionneurs » et les interfaces – ces ajouts électriques, mécaniques, sensoriels... qui rendent pourtant ces objets « intelligents », capables de comportements autonomes et/ou relationnels. ». Par ailleurs, l'auteur relève la parenté de cette notion avec ce qu'il nomme des « grands récits fédérateurs » marqués par leur incompatibilité respective et dans l'Intelligence Ambiante (AmI) fait partie. Celle-ci serait fondée sur le développement des espaces et des services, le Machine to Machine (M2M) sur celui des organisations et des processus, le Réseau et société ubiquitaire (U-Society) sur l'entente des humains et des machines, la société de surveillance sur l'aliénation des consommateurs aux pouvoirs.

Cependant, en complétant cet examen de la nature du projet par la forme d'organisation qu'il emprunte, l'analyse montre que le projet répond à un autre mode d'anticipation non directement concurrent du mode adaptatif, le « *mode d'anticipation opératoire* ». Sous catégorie de ce mode, les « *anticipations de type flou* » ou « *partiellement déterminées* »<sup>217</sup> correspondent ici au caractère exploratoire du projet COPRIM (voir la dernière ligne du Tableau 6).

Ainsi, la division du travail par lots (*workpackages*) incluant des tâches répondant à des objectifs déterminés et des sous-tâches relatives, le tout en ayant pour horizon une finalité commune (la réalisation d'un démonstrateur), auraient pu nous inciter à comprendre le projet comme fondé sur un « *mode d'anticipation opératoire de type rationnel* ». Cependant, et une fois encore, les frontières analytiques semblent ne pas résister à la nature protéiforme des projets exploratoires. Le projet COPRIM est organisé selon le mode de la gestion par projet<sup>218</sup> avec une structure hiérarchique identifiée (chef de projet, responsables de lots, de tâches et de sous-tâches). Ce mode de gestion est une innovation contemporaine de la seconde guerre mondiale dont l'acte mythique de création est conté par l'histoire du *Manhattan Project* d'où sera issue la première bombe atomique, sous l'impulsion du Président Roosevelt. Avant de s'étendre aux différents secteurs de l'ingénierie civile de la recherche appliquée et du développement technologique, le mode de gestion par projet s'est développé dans les domaines militaires et de l'aérospatiale. Son succès précoce a même causé son identification avec la démarche de « Recherche-Développement » comme le note Auvray (1975).

<sup>217</sup> Boutinet les définit ainsi : « [...] à travers le projet, il s'agit de faire advenir pour soi un futur désiré ; dans sa perspective opératoire, le projet ne peut porter sur le long terme trop conjectural ; il ne peut non plus se limiter au court terme trop immédiat. Son caractère partiellement déterminé fait qu'il n'est jamais totalement réalisé, toujours à reprendre, cherchant indéfiniment à polariser l'action vers ce qu'elle n'est pas. Plus que le plan, l'objectif ou le but, le projet avec sa connotation de globalité est destiné à être intégré dans une histoire, contribuant autant à modaliser le passé qui est présent en lui qu'à esquisser l'avenir. C'est dire que tout projet à travers l'identification d'un futur souhaité et des moyens propres à le faire advenir se fixe un certain horizon temporel à l'intérieur duquel il évolue. Mais ce projet ne s'arrête pas à l'environnement dans son évolution prévisible. Il concerne d'abord l'acteur qui, présentement, se donne lui-même une perspective pour l'avenir qu'il souhaite. Nous le définirons donc comme une anticipation opératoire, individuelle ou collective d'un futur désiré. » (Boutinet, 2007 p. 67)

<sup>218</sup> « La gestion par projet se veut être un mode original de gouvernement qui vise à déterminer les meilleures conditions dans l'implantation d'une innovation au sein d'un ensemble organisationnel, qu'il s'agisse d'une innovation technologique, d'une innovation comptable, d'une innovation sociale... » (Boutinet, 2007 p. 220). « *Le project management* en conclusion est un essai de combinaison de ressources humaines et de paramètres techniques qui sont associés dans le même ensemble au sein d'une organisation « temporaire » pour réaliser un dessein spécifique. Cette combinaison implique une mutuelle concession au sein de l'entreprise entre départements fonctionnels et départements opérationnels chargés de la mise en place du projet. » (Boutinet, 2007 p. 223-224)

Tableau 6. Les modes d'anticipation (Boutinet, 2007)

Modes d'anticipation	Figures de l'anticipation	Conceptions liées à l'anticipation
<b>ADAPTIF</b> - De type empirique - De type scientifique	{ PREVOYANCE PREVENTION PREVISION	CONJECTURE PREDICTION CONJECTURE/PREDICTION
<b>COGNITIF</b> - De type occulte - De type religieux - De type scientifique ou philosophique	DIVINATION PROPHETIE { PROSPECTIVE FUTUROLOGIE	PREDICTION/DESTIN PREDICTION/DESTINEE CONJECTURE CONJECTURE
<b>IMAGINAIRE</b> - De type imaginaire rationnel - De type imaginaire onirique	UTOPIE SCIENCE-FICTION	AVENIR AVENIR
<b>OPERATOIRE</b> - De type rationnel - De type volitif formel	{ BUT OBJECTIF PLAN VŒU { SOUHAIT PROMESSE	DEVENIR DEVENIR DEVENIR MIXTE MIXTE MIXTE
- De type flou	PROJET	DEVENIR

Nous avons vu auparavant que le projet COPRIM participait d'un mode d'anticipation adaptif à la nature double (de type empirique et de type scientifique) et que son organisation relevait d'un mode d'anticipation opératoire.

La combinaison de ces deux modes d'anticipation participe de la tension existant entre l'exploration et l'exploitation (March, 1991), entre la *poiésis*<sup>219</sup> et la *praxis*, tension qui caractérise l'ensemble des projets technologiques en tant que projet de transformation du réel et de création d'un ordre à venir :

*« En milieu technologique, le projet toujours ordonné à la poiésis est en même temps un élément de la praxis considérée dans ses liens avec le réel : c'est l'intention d'une transformation du réel ; c'est l'intention d'une maîtrise toujours plus poussée que l'homme tente de l'ordre capricieux de la nature. Une telle praxis constitue sans doute la face positive du projet. Cette face fait de ce dernier le moyen privilégié pour assurer un possible progrès qualitatif. Mais il est une autre face, celle-là négative et souvent dissimulée qui,*

<sup>219</sup> A ne pas confondre avec la pratique poétique de l'usage évoquée dans la première partie.

*devant les désillusions de la croissance, cherche à travers le projet la façon par laquelle redonner du sens, lutter contre l'absurde. » (Boutinet, 2007 p. 73)*

Cet ordre à venir, qui s'incarne dans la foi en l'avènement de l'Intelligence Ambiante, est donc un ordre dans lequel le projet se présente comme une contribution. Ici, c'est par une tournure tautologique que le projet prend tout son sens : le projet, en tant qu'anticipation adaptative, existe car l'Intelligence Ambiante *va* exister. Dès lors, la gestion de projet peut être adoptée comme mode de gouvernance car elle permet de comprendre l'innovation dans la continuité d'un à-venir prévisible. L'enthousiasme technologique permet à la fois de donner sens au projet et à son mode de gestion en les ancrant dans une logique plus innovante que créatrice<sup>220</sup>.

## ***B - La sécurité au cœur de l'intrigue technologique***

Comme l'explique Boutinet, l'équipe-projet se fixe comme objectif la résolution originale d'un problème unique et commun à l'ensemble de ses membres :

*« L'organisation à projet est mise en place pour nous éloigner de la routine, pour particulariser les situations, re-personnaliser les êtres et les choses : chaque projet entend justement se confronter à un problème qui se veut unique, qui est à résoudre de façon inédite. Pour le résoudre, la gestion de projet va constituer une organisation ad hoc : on réunit un groupe pour concrétiser et implanter une innovation puis on le disperse une fois que le travail est réalisé, ou que pointe l'opportunité d'une nouvelle innovation jugée plus importante. » (Boutinet, 2007 p. 247)*

On comprend que la réalisation du processus de problématisation, plus qu'un objectif, est la raison d'être du projet. Une correspondance existe entre le problème posé, les solutions envisagées et la composition de l'équipe-projet. Analytiquement, cela a des conséquences sur le regard porté sur l'équipe-projet : il faut se départir de la considérer

---

<sup>220</sup> « Le projet technologique à travers la gestion des organisations et les initiatives mises en place pourrait être assimilé à deux logiques différentes, sans que l'on sache très bien laquelle prédomine aujourd'hui, une logique des héritiers, une logique des bâtisseurs ; les héritiers doivent se soucier de faire fructifier d'anciens projets forgés en amont d'eux en apportant leur contribution à travers leurs propres objets ; cette logique des héritiers ne peut en effet se limiter aujourd'hui à maintenir simplement ce qui existe, à moins de menacer de régression leur entreprise confrontée à d'inéluctables changements ; il lui faut au contraire continuellement chercher à développer, adapter, diversifier. C'est sans doute en ce sens que l'on pourrait penser l'innovation du projet d'entreprise ou de la gestion par projet. Les bâtisseurs en ce qui les concerne donnent au contraire l'impression d'opérer une rupture par rapport à l'amont qui se trouve ainsi relégué, rejeté ; ils se lancent dans un effectif projet d'entreprendre qui au-delà de l'innovation se veut véritable œuvre de création. [...] la création se fait transgression alors que l'innovation se veut continuité ; le créateur devient ainsi en quelque sorte sa propre transcendance alors que l'innovateur trouve la transcendance dans l'outil existant qu'il cherche à transformer. » (Boutinet, 2007 p. 248-249)

comme une équipe amenée à résoudre un problème (« *problem-solver* ») et l'appréhender comme un faisceau de solutions socio-techniques *ad hoc*, un « *bundles of solutions* » :

*« Clearly, one of the major lessons that scholars of technology can borrow from the sociology of scientific knowledge is an awareness of how scientists and inventors construct both nature and explanations of nature. To apply this to technology, it is useful to think about inventors not as problem-solvers but instead as bundles of solutions who construct problems suited to their unique skills and ideas. [...] Yet inventors are not just bundles of technical solutions; they are also bundles of social solutions. Inventors succeed in a particular culture because they understand the values, institutional arrangements, and economic notions of that culture. »* (Carlson, 1992 p. 175)

Dès lors, la situation est rendue problématique par le faisceau de solutions sociotechniques en présence dans le projet. C'est à partir de la constitution de ce faisceau que l'analyse doit partir pour appréhender le dimensionnement et la nature du problème. Le succès du projet repose ainsi sur l'articulation de chacune des composantes du faisceau. Nous verrons, en premier lieu, la manière dont la sécurité informationnelle s'articule au faisceau de solutions disponibles dans le projet (a) avant de nous saisir de la technologie NFC pour mieux comprendre comment celle-ci dynamise l'inscription de la projection d'usages dans l'enthousiasme technologique (b).

## **1) Articuler la sécurité au faisceau de solutions**

Pour ce faire, nous proposons de convoquer les travaux de Vinciane Despret (2002). La philosophe étudie les modifications de notre conception de la nature et des hommes en fonction des mutations politiques, religieuses et sociales du monde. Se référant aux innovations méthodologiques de l'éthologue Thompson<sup>221</sup>, qui a travaillé sur le comportement des primates, elle démontre que celles-ci ont produit des résultats qui ont pêchés par exotisme pour être estimés scientifiquement valides par les chercheurs contemporains de l'époque. Les observations de Thompson, qui prenaient place en dehors du cadre du laboratoire, posaient problème par leur non-reproductibilité et les résultats scientifiques obtenus étaient donc critiqués pour leur manque de robustesse :

*« L'animal pourra plus tard raconter des histoires très similaires, mais, pour devenir robuste, il devra être soumis au régime de la preuve : l'extraordinaire n'a pas sa place dans*

---

<sup>221</sup> Thompson, Edward Pett, 1851, *The Passions of Animals*, London, Chapman & Hall

*les sciences, à moins de se répéter – et donc de perdre son statut exceptionnel. Les études de terrain beaucoup plus longues et les expérimentations en laboratoire seront les modes par lesquels cette répétition exigée pourra avoir une chance d’advenir. » (Despret, 2002 p. 100)*

Pour Vinciane Despret, ce qui a fait défaut à Thompson n’est pas tant le manque de rigueur de son dispositif méthodologique que l’articulation de sa méthode à l’ethos contemporain de la science. Autrement dit, le faisceau de solutions méthodologiques mis en place par l’éthologue était mal « articulé » à la manière de poser scientifiquement le problème de l’observation des primates.

Dans notre cas d’espèce, l’articulation du faisceau au problème trouve sa résolution dans la définition d’un problème abordable par les parties au projet. Si le « singe » à observer doit nécessairement être un « *singe* » de laboratoire, dans le cadre du projet, le problème à traiter doit nécessairement être un problème appartenant à « la sphère technique ».

Ainsi, la distinction effectuée par le chef de projet entre « attaques en labo » et « attaques dans la rue »<sup>222</sup> ne doit pas nous induire en erreur. Si le cadre de l’intrigue s’inscrit bien dans une écologie socio-technique urbaine, l’intrigue elle-même est centrée sur la construction de mécanismes de défense à ces attaques sur l’information échangée. C’est l’objet du projet de concevoir un « Contactless Privacy Manager ». Les premiers échanges qui ont eu lieu lors du **Comité de pilotage 1 (T0)** vont confirmer ce qui figurait en filigrane dans l’annexe technique au projet. C’est moins la notion floue de « Privacy » qui est considérée comme problème que la notion de sécurité. C’est d’ailleurs le titre de l’axe thématique de l’ANR auquel le projet appartient : « Sécurité pour les télécommunications et les réseaux. » L’objectif principal du projet est ainsi décrit en ces termes dans l’annexe technique :

*« The main goal of the project is to secure from relevant threats the transfer of private data information to and from contactless portable devices that communicate within the near field component of the electromagnetic field. » (Annexe technique/annexe 4)*

En somme, si la « Privacy » retient l’attention de l’équipe-projet, c’est parce que sa protection est envisagée comme problématique dans le contexte d’un déploiement rapide des technologies sans contact. Le succès de ces technologies, *taken for granted*, fonde la pertinence de l’orientation technologique de la question à adresser :

<sup>222</sup> « Enfin, dans la lignée des discussions sur les scénarios d’attaque, le CEA-LETI (chef de projet) a précisé qu’il y a deux types d’attaques : « celles dites *en labo* pour lesquelles la question de la Privacy n’est pas bien cernée et celles dites *dans la rue* qui, semble-t-il, devraient avoir la priorité dans le projet. Il faut qu’on s’accorde dessus lors du prochain copil de septembre. » Voir chapitre VII.h)

*« Cependant une certaine inquiétude s'est faite jour auprès des utilisateurs de la technologie sans contact concernant la protection de la vie privée. En effet ces systèmes sans contact peuvent être potentiellement l'objet d'actions malveillantes cherchant à mettre en défaut de façon consciente ou inconsciente la confidentialité des données échangées. En outre la caractéristique des objets sans contact est que ces actions peuvent avoir lieu sans que le propriétaire de l'objet en soit informé, donc à son insu. Sans mesures de protection particulières le concept d'Intelligence Ambiante peut tracer quelqu'un. »* (Annexe technique)

Ainsi, tandis que plusieurs dimensions du problème sont présentées dans l'annexe technique<sup>223</sup>, le cœur du problème est foncièrement technologique. La situation problématisée participe d'un certain déterminisme technologique : puisque les technologies sans contact vont se diffuser et que cette technologie présente des failles en matière de sécurité, il faut combattre ces menaces par l'apport de technologies adaptées. Dans cet ordre d'idée, l'exploration de pistes de conception qui ne s'inscrivent pas directement dans cet à-venir technologique est écartée<sup>224</sup>.

On comprend ainsi que la « *Privacy* » ne constitue pas le cœur du problème. La notion ne peut néanmoins pas être simplement évacuée du projet, comme participant d'un problème inhérent à la sphère sociale, car, comme la sécurité, elle est consubstantielle de la thématique de l'Intelligence Ambiante :

*« Security and Privacy are a 'penultimate slide' problem for ubiquitous computing—the second to last slide in many conference presentation notes that there are security or Privacy problems with the system that has been described, and that future work will address these issues. The “penultimate slide” syndrome indicates two things—first, that security and Privacy issues are centrally implicated in the future success of ubiquitous computing, and, second, that they are currently poorly understood. »* (Dourish, Grinter, Delgado & Joseph, 2004)

Comme nous l'avons annoncé auparavant, l'un des moyens de surmonter cette difficulté est la *technologisation* de la « *Privacy* » par sa transformation en un problème de sécurité. Cela s'effectue dans un premier lieu par la stabilisation<sup>225</sup> de la notion de

<sup>223</sup> Elles sont scindées en plusieurs « challenges » dans le plan de l'annexe : scientifique, technical, economic and technical challenge. Voir annexe 4

<sup>224</sup> En effet, elle a exprimé ses réserves sur le fait d'avoir à entamer le travail de scénarisation sans aucune idée de l'aspect du CPM si celui-ci devait être un « stand-alone » dispositif. Umanlab a évoqué la possibilité d'explorer des pistes de développement technologique non réalisables immédiatement, le CEA-LETI a répondu qu'il est réticent à « faire du travail pour rien ».

<sup>225</sup> « The degree of stabilization was introduced as a measure of the acceptance of an artifact by a relevant social group. The more homogeneous the meanings attributed to the artifact, the higher is the degree of stabilization. [...] These stabilization

« *Privacy* », dont le caractère fuyant de la définition est reconnu (Agre & Rotenberg, 1998 ; Ariès & Duby, 1999 ; Etzioni, 1999 ; Sirey, 2007), en évacuant ce pour quoi le faisceau de solutions n'est pas compétent. Au départ, le scénario, bien qu'encore à l'état de concept, comprend une multitude de formes d'existence de l'utilisateur. L'humain est alors un attaquant, un utilisateur, un client, compris comme agissant de manière rationnelle (motivations économiques) ou « pour le fun » (chef de projet). C'est une entité floue. Tandis que sa définition formelle ne constitue pas alors une priorité, l'intrigue qui doit s'inscrire au cœur du scénario est dictée par l'impératif de répondre à la sécurisation de l'information échangée. Le scénario doit impérativement mettre en scène des « menaces », « attaques » et « parades » du système d'information, toutes devant faire l'objet d'une évaluation comparative. Cette première phase de stabilisation de l'intrigue a duré sept mois, période durant laquelle ont eu lieu neuf réunions multipartenaires. Ainsi, l'on peut distinguer deux sources distinctes qui nourrissent le scénario. D'une part, l'intrigue s'organise à partir d'une lecture technologique de la sécurité de l'information. D'autre part, l'autre source d'information est constituée par l'environnement au sein duquel se déroule l'intrigue. Cette scission des sources de création du scénario participe du caractère déjà hybride de celui-ci : tandis qu'une dose de créativité *extrascientifique* semble autorisée pour l'élaboration de l'environnement, cette créativité est bornée par l'intrigue au cœur des scénarios. Le scénario est d'abord un lieu où se joue la résolution d'une « menace » pesant sur la sécurité de l'information. Il appartient alors aux représentants des usagers de renseigner le consortium sur les règles du jeu en vigueur dans l'environnement de cette « menace ». Cependant, la caractérisation de la menace va rejaillir de manière inattendue sur la nature et la fonction originellement prévues pour le scénario.

Ainsi, lors du **Comité de pilotage 4 (T0 + 11)**, les critiques de la doctorante de l'UVSQ concernant le manque de « *Privacy* » dans les scénarios sont évacuées et ne seront plus jamais discutées. La notion de « *Privacy* », bien que faisant l'objet d'un travail en cours d'état de l'art mené par Umanlab, est définie et verrouillée par le CEA-LETI et par l'UVSQ avec un prisme technique durant le **Comité de pilotage 2 (T0+3)**. Pour les uns, c'est une notion antagoniste de celle de sécurité, tandis qu'en cryptologie, la notion est considérée comme n'existant pas en tant que telle. En somme, une partie du faisceau de solutions considère la « *Privacy* » comme un problème résidant au-delà de leur champ de compétences car hors de la sphère technique. Néanmoins, il nous faut encore expliquer la

---

processes have a dual character: They include irreversible processes of closure that impose a steplike character onto technical change, but they are also continuous in-between, as is described by growing and diminishing degrees of stabilization. » (Pinch, 1993 p. 121)



survivance de la notion dans le projet par deux phénomènes concourants : la *technologisation* de la « *Privacy* » s'effectue par son assimilation à la notion de sécurité et par l'inscription de cette version technologisée du concept dans les scénarios.

L'évènement que nous avons qualifié de déstabilisateur<sup>226</sup> est représentatif du mouvement de technologisation de la « *Privacy* ». Celle-ci y est considérée, au miroir de la sécurité (voir ci-dessous) comme une donnée quantifiable. Ce mouvement va peu à peu enclencher une assimilation de la « *Privacy* » à la sécurité comme l'atteste cet extrait de compte-rendu de réunion, rédigé par le CEA-LETI : « l'UVSQ a fait une présentation sur les aspects protection de la vie privée et comment des derniers sont pris en compte et formalisés au niveau protocolaire. » **Comité de pilotage 3 (T0 + 8)**

D'autre part, ceux sont les différentes options de sécurisation de l'information qui sont placées au cœur de l'intrigue des scénarios (cf. **Conférence téléphonique (T0 + 15)** en vertu de l'analyse de la sécurité présentée par l'UVSQ<sup>227</sup>. L'intégration de la « *Privacy* » dans les scénarios est également freinée par l'incapacité d'une partie du faisceau de solutions, Umanlab, à fournir une robustesse convaincante au « social ». Dépourvus de « *prises* » (Bessy & Chateauraynaud, 1995) avec celui-ci<sup>228</sup>, les autres membres du projet n'ont d'autre choix, pour l'articuler avec le problème, que de le *technologiser*. A défaut, le problème se trouve évacué ou ne sert que de canevas contextuel à l'intrigue<sup>229</sup>. A titre d'exemple, le rôle du CEA-LETI consiste à « chercher à mettre de l'innovation dans des produits et donc de l'électronique » selon le chef de projet. Dans ce cadre, les scénarios sont définis par le chef de projet comme étant un « ensemble de menaces, de moyens à mettre en

<sup>226</sup> « J'aimerais que l'on se rencontre entre voisins pour faire un point sur les différents scénarios induisant des pbs de Privacy avant le prochain COPIL et la conf call. En particulier, il serait bien de déterminer dans chacun de nos scénarios une échelle de dangerosité (si c'est possible, à discuter !)... une sorte de mesure de la perte de Privacy. » (Cf. L'évènement déstabilisateur (T0 + 5 ½))

<sup>227</sup> « Dans sa présentation sur l'état de l'art des attaques protocolaires et des modèles de sécurité, l'UVSQ a défini en quoi consistait une analyse de la sécurité (« For each considered protocol, give cryptographic security arguments telling which security requirements are fulfilled by using a security proof and which are not by showing an attack »). Ainsi la notion de sécurité reflétait une menace qui impliquait d'identifier les buts de l'attaquant et un modèle de déroulement de l'attaque. Ainsi, la preuve de sécurité se démontrait de deux manières : soit en essayant de monter une attaque (si l'attaque réussit, le système n'est pas sûr ; si elle échoue, rien ne peut être affirmé), soit en prouvant qu'aucune attaque n'est réalisable sous certaines conditions. En réponse à une question de Umanlab, l'UVSQ a affirmé que la séparation entre la couche physique et la couche protocolaire est analytique mais « qu'en réalité, les deux sont mêlées. » (VII.B - b)

<sup>228</sup> « Lors de la réunion avec l'un des membres du CEA-LETI, celui-ci a présenté l'attaque en relais comme celle sur laquelle les scénarios doivent se concentrer. La priorité, pour le projet, était d'aboutir à l'évaluation des risques. Après avoir fait l'effort de nous expliquer chacune des attaques en des termes plus accessibles, moins techniques, notre interlocuteur a admis considérer que les aspects sociaux, économiques et légaux en lien avec la problématique lui étaient complètement étrangers. Dès lors, il ne pouvait que nous dire les attaques sur lesquelles on doit s'attarder. » Réunion CEA-LETI/Umanlab (T0 + 4)

<sup>229</sup> « Le doctorant d'Inside et moi-même avons présenté le document « Payment » consolidé. Les premières remarques ont porté sur le mode de fonctionnement du lien sans contact et des imprécisions liées dans le document. Le CEA-LETI a demandé à ce que le mode de fonctionnement soit précisé « car s'il est en ISO 14443 ou ISO 15693 ou Peer to Peer actif, les menaces et vulnérabilités sont pas du tout les mêmes ! ». Par ailleurs, nos interlocuteurs ont apprécié d'avoir vu apparaître le terme confiance dans l'analyse « sociologique » mais notent deux facteurs importants à prendre en compte : la sécurité du point de vue des opérateurs et le possible surcoût industriel des solutions proposées. » (VII.C - e) .

œuvre pour attaquer la sécurité des communications et du coût de la protection à mettre en place ». Une distinction nette est établie par le CEA-LETI entre les « peurs fondées » et les « peurs fantasmées » par l'utilisateur. Prenant une posture rationaliste affirmée, le chef de projet précise que l'objectif du projet n'est d'abord que les premières, c'est-à-dire les peurs reposant sur « des menaces technologiques pertinentes », les autres devant être résolues par le biais d'une communication efficace. L'aveu du chef de projet est en ce sens éloquent lorsqu'il évoque l'association des SHS au projet :

*« Parce que, à l'époque, tout à fait, c'est l'ANR qui nous l'a suggéré. Parce qu'à l'époque, il ne m'est pas venu à l'idée que dans un projet, on va dire, technologique, on puisse introduire d'emblée, un partenaire SHS. C'est, la connexion n'était pas faite à l'époque. »* (Entretien SHS/innovation : interview du chef de projet)

Cette articulation du faisceau au problème de la sécurité est d'autant plus compréhensible lorsque l'on se penche sur le traitement scientifique de la notion. La question de la sécurité informationnelle (« *information security* ») bénéficie d'une attention large dans plusieurs champs scientifiques et technologiques<sup>230</sup> : l'électronique, la cryptologie, l'informatique, la recherche et l'ingénierie en systèmes d'informations sont les principales disciplines contributrices. Cependant, l'exercice de l'interdisciplinarité est limité à un accord qui transcende les champs académiques et professionnels. Il s'agit de l'importance unanimement accordée aux quatre conditions à respecter pour assurer la sécurité de l'information :

- 1- L'intégrité : l'information ne doit pas être modifiée par l'intervention d'un tiers non autorisé
- 2- La disponibilité : l'information doit être disponible lorsque demandée par des sujets autorisés
- 3- La confidentialité : la divulgation irrégulière de l'information doit être détectée et empêchée.
- 4- L'authenticité : les données, transactions, documents, communications et les parties œuvrant lors de la communication doivent être authentiques.

Siponen & Oinas-Kukkonen (2007) ont démontré que ce fond commun et interdisciplinaire permettait de résumer à quatre les questions que se posent chercheurs et ingénieurs en matière de sécurité informationnelle :

---

<sup>230</sup> L'analyse qui suit est essentiellement fondée sur un état de l'art critique et interdisciplinaire de (Siponen & Oinas-Kukkonen, 2007)

- 1- L'accès au système d'informations : comment l'accès des individus à l'information peut-il être contrôlé ?
- 2- La sécurisation de la communication : comment une communication sécurisée entre les individus peut-elle être assurée ?
- 3- La gestion de la sécurité : comment la sécurité de l'information doit-elle être gérée ?
- 4- Le développement d'un système d'information sécurisé : comment un système d'informations doit-il être développé afin d'être sécurisé ?

Notre objectif ici n'est pas de discuter la pertinence de ce cadre analytique<sup>231</sup> mais de tirer parti des conclusions de leur analyse pour étayer notre argument. Les auteurs en tirent une leçon et trois conclusions. D'abord, les recherches sont essentiellement centrées sur la résolution de problèmes techniques tandis que les aspects conceptuels et organisationnels bénéficient d'une attention moindre, sinon nulle. Ainsi, les questions privilégiées sont celles de l'accès au système d'information (SI) et celle de la sécurisation de la communication. Or, ces deux questions privilégient des approches mathématiques et engagent des disciplines différentes seulement de manière marginale. Cette emphase sur la résolution technique des problèmes a trois conséquences. Premièrement, l'introduction de solutions technologiques pose mécaniquement celle de l'adoption de celles-ci par les utilisateurs. La seconde est que nombre de recherches sont exclusivement envisagées par l'apport de solutions techniques alors qu'elles concernent des problèmes plus larges et complexes. Enfin, les auteurs soulignent l'absence de revues de littérature critiques et pluridisciplinaires et l'expliquent par le fait que la recherche pragmatique soit favorisée en raison de résultats réputés rapides et probants, une critique qui touche moins les cryptologues et les informaticiens. Dans le même sens, les approches qui ne sont pas fondées sur des modèles mathématiques ne sont souvent pas bien reçues. Les auteurs plaident pour un développement d'études empiriques abordant les questions du développement de systèmes d'information sécurisée et de la gestion de la sécurité. Ils expriment le besoin de lier ces études aux techniques quantitatives et qualitatives, à l'élaboration de théories comme à leur validation par l'empirie et enfin à l'élargissement substantiel du champ de références aux sciences humaines et sociales : psychologie, sociologie, sémiotique et philosophie.

<sup>231</sup> Nous notons néanmoins que le matériau sur lequel s'appuient les auteurs exclut tout ou partie des réflexions engagées dans le champ disciplinaire des interactions homme-machine (HCI), champ dans lequel les liens entre « Privacy » et sécurité ont fait l'objet de travaux significatifs. Sans prétention d'exhaustivité, on pourra consulter à cet égard : (Bellotti & Sellen, 1993 ; Clement, 1994 ; Bellotti, 2001 ; Langheinrich, Marc, 2001 ; Samarajiva, 2001 ; Lederer, 2003 ; Leysia & Paul, 2003 ; Palen & Dourish, 2003 ; Dourish, Grinter, Delgado & Joseph, 2004 ; Langheinrich, M., 2005)

Les résultats de cette étude sont très instructifs lorsque rapportés à notre cas d'espèce. D'abord, ils permettent de toucher du doigt le caractère dynamique de la problématisation de la sécurité. Celle-ci n'était pas acquise mais a été construite par la remise en cause de la « Privacy » et par le travail de « *définition de la situation* » de chacun des partenaires. Contrairement à la « Privacy », la sécurité offre une assise théorique unifiée, quantifiable et significative d'un point de vue technique<sup>232</sup> :

*« The way that scientists tell which differences are significant and which are irrelevant in part depends upon their theories and background assumptions or the ceteris paribus clauses assumed in the production of any experimental result. The background theories and assumptions, especially when a new phenomenon is claimed, are often themselves far from straightforward to elicit, as they are embedded within the very experimental claims at issue. In short, similarity and difference relationships are constituted within a wider framework of culture and action are at the very heart of how truth and falsehood are established in science. »* (Pinch, 1993 p. 31)

Cette stabilisation de l'intrigue autour de la question de la sécurité informationnelle octroie à celle-ci un caractère d'« *inévitabilité* »<sup>233</sup>. Autrement dit, les choses sont présentées de telle sorte qu'il n'y ait pas d'autre moyen que celui-ci d'envisager le problème.

## 2) Articuler le NFC comme paradigme technologique

Revenons brièvement aux travaux de Vinciane Despret et aux aventures de l'éthologue Thompson pour introduire cette partie. En s'inspirant de la théorie de l'acteur-réseau (Akrich, Callon & Latour, 2006), Vinciane Despret ajoute une autre raison à l'échec de Thompson à convaincre ses contemporains. Il s'agit du manque d'alliés articulés au « *singe* ». Pour qu'il en ait eu, il eut fallut que des articles, des expériences, des réseaux de chercheurs, des organismes financiers contribuent à la stabilisation et à la socialisation des singes par la communauté scientifique :

*« Ces singes sont mal articulés dans le sens où ils n'ont pas réussi à se lier à un nombre d'intérêts suffisants, à devenir le site d'agencements de préoccupations de nombreuses personnes et de questions importantes à poser. »* (Despret, 2002 p. 101)

<sup>232</sup> « Scientists are, of course, in constant, intimate dialogue with the real, material world, but they are active participants in that dialogue, bringing to it conceptual schemas, experimental traditions, intellectual investments, ways of understanding the world, models and metaphors – some drawn from the wider society – and so on. » (MacKenzie & Wajcman, 1999 p. 7)

<sup>233</sup> « Once a fact or artifact has become black-boxed, it acquires an air of inevitability. It looks as though it is the best or only possible solution to its set of problems. » (Sismondo, 2004 p. 4)

Dans notre cas, considérer la problématisation comme un processus d'enrôlement est d'autant plus judicieux que l'on s'intéresse à l'étendue de la projection en dehors du réseau local existant (le projet). Ainsi, le problème de la sécurisation des données est audible car le faisceau de solutions s'est donné un moyen précieux de l'inscrire à portée raisonnable de l'horizon technologique. Cette portée raisonnable est le NFC et les promesses qui y sont associées. Travailler sur le NFC, c'est en somme se donner une ressource légitime pour l'action de conception.

Il nous faut tout d'abord considérer cette technologie comme le « *paradigme technologique* » (MacKenzie & Wajcman, 1999) de la réflexion sur la sécurité que doit mener l'équipe-projet. Dérivé du concept original Kuhnien<sup>234</sup>, le concept de « *paradigme technologique* » souligne la diversité des productions technologiques fondées sur un paradigme identique<sup>235</sup>. Ainsi, le concept de « *paradigme technologique* » nous permet de comprendre le NFC non comme *une* technologie spécifique mais bien comme une *constellation de choses* qui entrent en cohérence pour une communauté donnée. Pour organiser notre exploration de cette constellation, nous avons choisi de reprendre la manière dont MacKenzie et Wajcman (MacKenzie & Wajcman, 1999) ont déplié la notion de technologie. La première couche sémantique renvoie ainsi aux objets physiques et artefacts et aux activités et processus associés (« le NFC comme allié »), la seconde couche fait écho à ce que les gens savent, font et projettent du NFC (« Les promesses du téléphone NFC »).

## *Le NFC comme allié*

La communication en champ proche (« Near Field Communication », NFC) est un standard technologique de connectivité sans fil et à courte portée entre dispositifs électroniques (PDA, téléphones, terminaux, etc.). Elle est dérivée de la technologie des cartes à puces sans contact<sup>236</sup>. Le NFC est fondé sur la technologie d'identification de fréquences radio (« Radio Frequency Identification », RFID) qui peut être divisée en deux grands champs : le champ éloigné (« far-field ») et le champ proche (« near-field »), ce dernier étant issu de développements menés à partir du premier. Exactement comme un

<sup>234</sup> Le paradigme est alors entendu comme « entire constellation of beliefs, techniques, and so on shared by the members of a given community. » (Kuhn, 1970 p. xii : 210)

<sup>235</sup> « [...] the paradigm is not a rule that can be followed mechanically, but a resource to be used. There will always be more than one way of using a resource, of developing the paradigm. Indeed groups of technologists in different circumstances often develop the same paradigm differently. » (MacKenzie & Wajcman, 1999 p. 10)

<sup>236</sup> Définie par le standard ISO/IEC 14443, les cartes à puces sans contact utilisent un couplage électrique pour réaliser la connexion. Pour fonctionner, la carte doit généralement être placée à proximité (<3 cm) du lecteur. Pour alimenter la carte, on utilise un couplage inductif ou capacitif. Par exemple : la carte navigo à Paris, les badges d'accès à certains bâtiments, etc.

lecteur de carte sans contact, un dispositif NFC radie un champ RF de très basse puissance de 13.56 MHz à partir d'une simple antenne enroulée. Les cartes à puces se couplent inductivement<sup>237</sup> à l'intérieur de ce champ par le biais de leur propre antenne. Ainsi, les cartes à puces n'ont pas de batterie embarquée et l'alimentation de ses propres circuits électroniques est assurée par l'absorption de l'énergie électrique émanant du champ RF. De manière liée, une fois ces circuits alimentés, la carte à puce peut donc recevoir et renvoyer des commandes et des données provenant d'un dispositif NFC ou d'un lecteur de carte<sup>238</sup>.

Ainsi, les systèmes NFC reposent sur deux éléments (cf. figure 33) :

- L'initiateur : initie et contrôle l'échange d'information (le lecteur)
- La cible : répond aux demandes de l'initiateur (la carte)

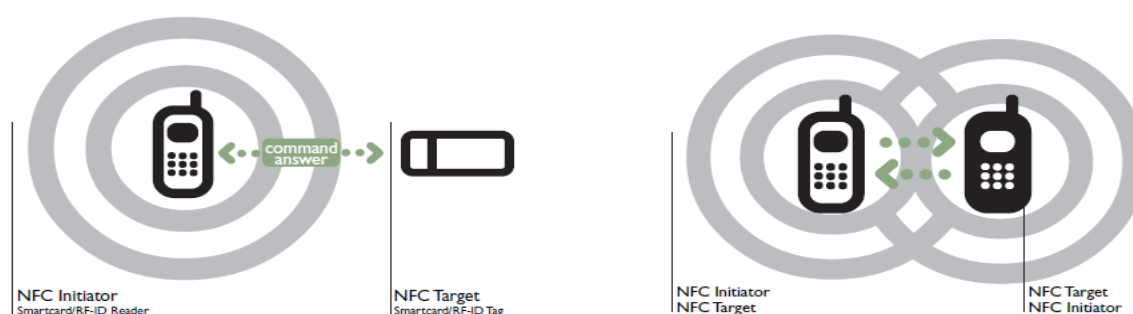


Figure 33. Modes de fonctionnement du NFC (Harold, 2005)

L'une des innovations majeures du NFC par rapport aux traditionnelles cartes à puces sans contact est la capacité d'une carte NFC à pouvoir jouer alternativement le rôle de carte ou de lecteur. Cette innovation inclut un mode de communication inédit dans lequel deux dispositifs NFC, chacun générant leur propre champ RF de 13.56MHz, peuvent établir une communication entre eux-mêmes. Il se dégage ainsi trois configurations de communications entre dispositifs (Figure 34) :

<sup>237</sup> « On appelle couplage le processus par lequel l'énergie du perturbateur atteint la victime. Dans le cas du couplage inductif, il existe dans le circuit perturbateur un courant susceptible de produire des perturbations. A proximité de ce circuit se trouve un circuit victime. Le courant du conducteur du circuit perturbateur produit autour de lui un champ magnétique. Ce champ magnétique induit un courant dans le circuit victime. »  
Source : [http://fr.wikipedia.org/wiki/Compatibilit%C3%A9\\_%C3%A9lectromagn%C3%A9tique#Le\\_couplage\\_inductif](http://fr.wikipedia.org/wiki/Compatibilit%C3%A9_%C3%A9lectromagn%C3%A9tique#Le_couplage_inductif)

<sup>238</sup> La commande et la transmission de données à partir d'un dispositif NFC ou d'un lecteur vers une carte sans contact est accomplie par une modulation d'amplitude sur le porteur de 13.56 MHz. Cependant, parce que la carte à puce a une puissance insuffisante pour générer son propre champ RF, elle renvoie les données au dispositif NFC ou au lecteur de carte en court-circuitant momentanément ses antennes de réception afin d'augmenter le chargement sur l'antenne de transmission du dispositif NFC ou du lecteur de carte. Ces changes de charges momentanés sont détectés par le dispositif/lecteur NFC, et le moment d'intervalle entre eux est utilisé pour décoder les données. (Harold, 2005)

Device A	Device B	Description
Active	Active	When a device sends data it generates an RF field. When waiting for data a device does not generate an RF field. Thus, the RF field is alternately generated by Device A and Device B
Active	Passive	The RF field is generated by Device A only
Passive	Active	The RF field is generated by Device B only

Figure 34. Configurations des communications entre dispositifs NFC (Harold, 2005)

Ces trois configurations de communication lorsque traduites en termes d'applications, permettent de distinguer trois modes d'utilisation du NFC (Haselsteiner & Breidfuss, 2006):

- Le mode carte : le dispositif NFC se comporte comme une carte sans contact. Les applications envisagées pour ce mode sont l'accès à des bâtiments sécurisés (parkings, bureaux, etc.), le paiement de transactions, l'identification d'individus, etc.
- Le mode lecteur : le dispositif NFC est actif et lit un tag RFID passif. Les applications projetées pour ce mode sont la lecture d'informations disponibles sur le mobilier urbain (posters, affiches), sur des objets personnels (photos).
- Le mode P2P (Peer-to-Peer) : deux dispositifs NFC communiquent ensemble et échangent de l'information. Les applications envisagées pour ce mode sont l'échange d'informations entre deux dispositifs (agenda, téléphone, configuration wifi, photos).

En tant qu'artefact, le NFC s'inscrit dans le champ de l'innovation en filiation avec une technologie déjà existante, la carte à puce sans contact (*contactless tag*). Celle-ci ne pouvait officier qu'en mode carte et dans un format de communication passif, tandis qu'un dispositif équipé du NFC peut agir selon le moment en mode carte ou lecteur, actif ou passif. Or, le problème de la sécurisation de l'information échangée, s'il repose sur des questionnements identiques pour la carte à puce ou le NFC, mérite une prise en compte des spécificités propres au NFC et notamment en termes de radiofréquences comme l'illustre cet extrait du **Comité de pilotage 2 (T0+3)** :

« Un court deuxième temps a été consacré à la présentation de solutions déjà existantes. Enfin, une proposition de fonctionnalités du CPM a été présentée, celui-ci n'étant alors intégré dans aucun dispositif technologique. Il est présenté comme un brouilleur empêchant des lecteurs non autorisés de lire des tags portés par l'utilisateur. Le chef de projet s'est interrogé sur l'identité même de l'objet : doit-il être « *stand-alone* » ou intégré au tag ? Une discussion s'est engagée entre Inside et le CEA-LETI sur le vocabulaire utilisé lors de cette présentation durant laquelle le CEA-LETI a indistinctement utilisé les termes « cartes sans contacts », « tags », « tags RFID ». Pour Inside, le NFC brouillait des catégories qui se distinguaient notamment par une séparation entre l'identification des personnes (contactless card) et traçage des objets (RFID) : « Le NFC est venu fausser cela et rapprocher les mondes » (Inside). Durant cette discussion, le CEA-LETI précise que le CPM était d'ores et déjà en cours de développement avancé. C'est un boîtier électronique qui « n'a rien de portable ». Il restait à l'adapter aux spécificités du NFC : « Le travail à faire dans COPRIM, c'est adapter le CPM au 13.56 [mhz], le NFC, quoi ! »

Ainsi, le travail sur le NFC transforme un problème éculé de sécurisation de l'information (celle de la carte à puces sans contact) en un défi d'avenir à relever par le faisceau de solutions présent dans le projet<sup>239</sup>.

### *Les promesses du téléphone NFC*

L'un des promesses majeures de la technologie NFC est le pont jeté entre monde virtuel et monde réel. En effet, cette technologie serait appelée à une intégration préférentielle au sein du dispositif mobile le plus populaire au monde, le téléphone mobile. Les analystes avaient prévu qu'en quatre ans (2007-2011), 500 million de téléphones portables seraient équipés de la technologie NFC (Csaposi & Nagy, 2007). Le rapport de (Falke *et al.*, 2007) nous éclaire sur l'implémentation sociale et économique du NFC. La recherche sur les téléphones équipés de la technologie NFC a reçu un soutien marqué à travers différents programmes (Chavira *et al.*, 2007) : Paypass de Mastercard, Visa Mobile et MobileJ/Speedy de JCB. Les auteurs résument les rapports des investigations concernées en deux points. En termes d'utilisation, le paiement, l'utilisation comme titre de transport

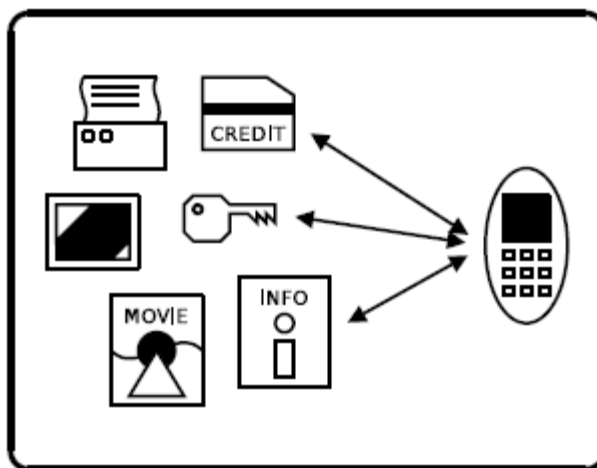
<sup>239</sup> « Existing technology is thus, we would argue, an important precondition of new technology. It provides the basis of devices and techniques to be modified, and is a rich set of intellectual resources available for imaginative use in new settings. But is it the *only* force shaping new technology? We would say that it is not, and would argue that this can be seen by examining the two most plausible attempts to claim that existing technology is more than just a precondition of new technology, but is an active force in its development. These attempts focus on the ideas of technological 'paradigm' and technological 'system'. » (MacKenzie & Wajcman, 1999 p. 9)



(« ticketing ») et le « smart poster » sont les applications les plus développées. Seule une application a fait l'objet d'un lancement commercial, à l'époque de la publication de l'étude, le « NFC-Handy Ticketing ». Lancée par une compagnie de transport public, la Rhein-Main Verkehrsverbund de la ville de Hanau, elle permettait aux clients d'utiliser les téléphones Nokia 3220 pour payer leurs titres de transport en portant leur téléphone à proximité des cibles placées dans les bus. A New-York, de janvier à Avril 2007, le programme « NYC Mobile Trial » a été porté. Il permettait aux utilisateurs de payer dans certains établissements, d'avoir accès à l'information à travers des posters intelligents (« smart posters ») et de payer pour leurs tickets dans les lignes de métro. La Philips Arena d'Atlanta en Georgie aux Etats-Unis a lancé un programme pilote dans lequel 150 détenteurs de tickets pour la saison de hockey et de basketball ont été équipés de Nokia 3220. Ils pouvaient les utiliser pour acheter dans les magasins, avoir accès à des vidéos et des images à travers des « smart posters » placés dans l'enceinte du stade. En novembre 2006 la Upper Austria University of Applied Sciences a engagé le projet « I want you » qui permet l'utilisation de téléphones NFC compatibles pour acheter dans les machines automatiques et dans les *coffee-shops* des campus. Ils fonctionnaient également comme des clés pour entrer dans les chambres et bâtiments.

L'association du NFC avec le téléphone augure donc d'usages de celui-ci comme portefeuille électronique comprenant des moyens de paiement, d'identification, des cartes d'accès, des informations diverses (voir Figure 35) et également de nouveaux services associés : mise en relation de dispositifs techniques, échanges de données entre dispositifs NFC (Benyo, Vilmos, Kovacs & Kutor, 2007).

*Figure 35. Le portable NFC comme portefeuille (Raitila, 2007)*



Cependant, cette union annoncée comme heureuse comporte deux zones d'incertitudes qui menacent la bonne entente attendue : les conflits portant sur la standardisation du NFC et le succès annoncé de l'adoption de la technologie.

L'intégration du NFC dans le téléphone mobile pose des problèmes de standardisation et de normalisation du fait des nombreux acteurs impliqués. Chacun d'entre eux espérant des gains supplémentaires de cette association, le processus de standardisation est le lieu de discussions techniques motivées par des intérêts économiques et politiques (Hawkins & Shea, 1995). Sans prétendre couvrir l'intégralité des enjeux, nous exposons ici un exemple de ces liens entre architecture du téléphone NFC et enjeux politiques. Dans la Figure 36, on peut observer trois éléments :

- à gauche le contrôleur NFC est un circuit intégré nécessaire à la conversion des signaux transférés à partir de la connexion avec un autre dispositif (lecteur RF, tag RFID/NFC ou dispositif équipé NFC). Il est « responsable » de la communication RF.
- Au centre, le contrôleur hôte est une carte d'extension qui règle les modes opératoires du contrôleur NFC et traite les données envoyées ou reçues par l'intermédiaire de l'interface HCI (« Host Controller Interface »).
- A droite, le *secure element* (élément de sécurisation), est un circuit intégré connecté au contrôleur NFC pour les transactions de proximité effectuées par le biais du SWP (« Single-Wire Protocole »). Il est « responsable » du stockage des informations sensibles. Le contrôleur hôte est également capable d'échanger des données avec l'élément de sécurisation.

Tandis que le NFC Forum<sup>240</sup> s'attaque à l'ensemble des détails fonctionnels du contrôleur NFC, les aspects liés à l'architecture du dispositif téléphonique ne sont pas abordés. Les opérateurs téléphoniques (GSMA) militent pour que la carte SIM joue le rôle d'élément de

---

<sup>240</sup> Tandis que les couches physiques et les liens logiciels ont déjà fait l'objet d'une standardisation par les organisations internationales agréées que sont ISO (International Organization for Standardization), ECMA International (European association for standardizing information an communication system<sup>240</sup>) et ETSI (European Telecommunications Standards Institute), le NFC Forum a été fondé dans l'objectif d'obtenir un accord sur les protocoles de données, les mesures de sécurité et sur les couches supérieures (Madlmayr, Ecker, Langer & Scharinger, 2008). Il a été fondé en avril 2004 par Nokia, NXP Semiconductors et Sony<sup>240</sup>. C'est un consortium d'industriels coopérant avec d'autres organisations de lobbying et de standardisation dont le but est la promotion de l'utilisation de la technologie NFC via le développement de spécifications, la garantie de l'interopérabilité entre dispositifs et services proposés et la communication de la technologie NFC (Forum, 2008). Il contient désormais cent cinquante membres actifs (fabricants, développeurs d'applications, institutions financières, etc.). Au premier semestre 2008, les membres du NFC forum étaient parvenus à trouver un accord sur les spécifications suivantes : les tags NFC doivent être lisible par n'importe quel dispositif NFC, le format d'échange de données doit être identique (NDEF) et sur quatre formats possibles d'enregistrement des données stockées dans les puces NFC. D'autres groupes de pression participent activement au travail de standardisation comme le Global System for Mobile Communications Association(GMSA), la communauté JAVA, la GlobalPlatform5 (GP) qui représente les intérêts de l'industrie des cartes à puces ou encore les associations de l'industrie financière.

sécurité (3) et que le Single-Wired Protocol (SWP) fasse lien entre le contrôleur NFC et l'élément de sécurité. La communauté JAVA participe également au travail de spécification des API<sup>241</sup> (JSR 177 et JSR 257 sur la figure). Ces API permettent de faciliter le développement d'applications à partir du NFC. Global Platform s'assure de son côté que l'intégration des cartes sans contact ne nuise pas à l'intérêt de ses membres tandis que les retombées attendues par l'industrie financière ajoute à la complexité technique de l'intégration du NFC dans le dispositif téléphonique. Ainsi trois points d'achoppement viennent contrarier ce travail de standardisation (Madlmayr, Ecker, Langer & Scharinger, 2008) :

- Le « OTA management » : OTA est un acronyme pour Over The Air. Cette technologie permet soit d'accéder aux données d'une carte SIM à distance, soit dans le cas du NFC, d'avoir accès à l'élément de sécurité. Tandis que l'on pourrait légitimement penser que la définition de l'OTA soit de la responsabilité des opérateurs mobiles (GSMA), d'autres organisations entrent en jeu dans la définition des standards, notamment l'OMA. En d'autres termes, aucun consortium n'a encore émergé afin de parvenir à un accord sur la gestion de l'OTA<sup>242</sup>. Par ailleurs, les auteurs signalent que l'absence de modèle économique robuste concernant les modes d'utilisation « *reader* » et « *peer-to-peer* », place l'élément de sécurité au centre du débat. Si celui-ci venait à se substituer aux cartes sans contact, les fournisseurs de l'élément de sécurité occuperaient une place clé dans l'écosystème NFC : baisse des coûts dus à l'inutilité de production de cartes à puces, vitesse de chargement de données supérieures, etc. Les opérateurs de téléphonie mobile ainsi que l'industrie financière sont extrêmement sensibles à ces débats.
- Des éléments de sécurité multiples : nous avons jusqu'ici évoquer l'élément de sécurité comme unique tandis qu'en réalité, les éléments de sécurité sont multiples et le travail de spécification pour la gestion simultanée et coordonnée de ces éléments n'est toujours pas abouti.
- La gestion de la puce (« tag management ») : la lecture de puces externes au téléphone mobile implique de nouveaux acteurs dans les négociations sur la standardisation. De nouveaux partenaires industriels responsables des dispositifs dans lesquels sont intégrées ces puces vont également devoir trouver un accord pour

<sup>241</sup> « Application Programming Interface », interface de programmation, indispensables à l'interopérabilité entre les composants logiciels.

<sup>242</sup> Rappelons que la création du NFC forum résulte de la volonté de partenaires industriels ayant indépendamment implémenté différentes versions de cartes sans contact dans les années 90.

assurer l'interopérabilité de celles-ci (c'est-à-dire la possibilité pour deux puces fabriqués par des opérateurs concurrents de dialoguer entre elles) mais également la sécurisation de l'utilisation.

Figure 36. Architecture d'une puce NFC intégrée dans un téléphone mobile (Madlmayr, Ecker, Langer & Scharinger, 2008)

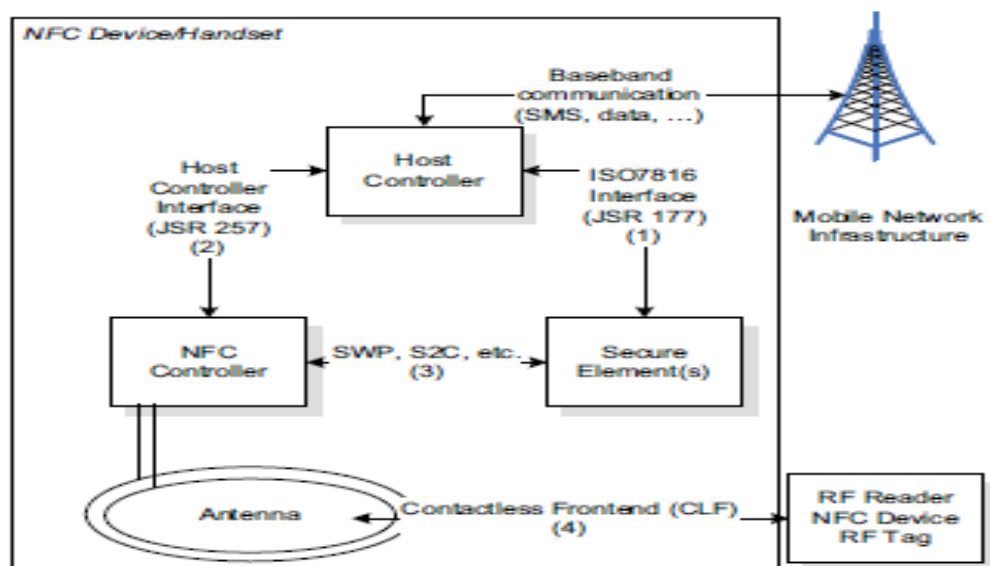


Figure 1. Architecture of NFC integrated in a mobile device.

Ces écueils qui pèsent sur la standardisation du NFC relativisent le caractère *dur* (« *obduracy* ») de ces alliés que constituent le téléphone et l'ensemble des processus qui y sont attachés. L'articulation est ainsi plus le fait d'un acte de croyance en l'à-venir que d'un fait avéré :

« [...] expectations constitute 'the missing link' between the inner and outer worlds of techno-scientific knowledge communities and fields. At the same time, expectations and visions are often developed and reconstructed in material scientific activities and disseminated in obdurate and durable forms. In a sense, expectations are both the cause and consequence of material scientific and technological activity. » (Borup, Brown, Konrad & Lente, 2006 p. 285)

Dans le cadre du projet, cette incertitude émerge dans les discussions dès l'émergence des premières ébauches des scénarios lors du **Comité de pilotage 5 (T0 + 13)** :

« Le CEA-LETI a présenté un état d'avancement du travail effectué concernant les attaques tandis qu'Inside a présenté le document rédigé avec l'aide de l'UVSQ sur les scénarios. Une discussion s'est engagée sur ce premier scénario (« Payment ») et particulièrement autour des particularités propres à chaque option technologique présentée. Inside a précisé que la première option était peu réaliste en raison de la clé cryptographique utilisée : « les clés statiques permanentes ont peu de chances d'être implémentées, ici. » Pour le deuxième cas, une argumentation technique est également développée en différenciant deux facteurs de génération de clés cryptologiques. Le responsable projet Inside a précisé que l'une était privilégiée par les Etats-Unis tandis que l'autre avait les faveurs de l'Europe. Concernant la troisième option technologique, le code PIN, Inside a affirmé que « cela n'est pas fait sur le NFC mais c'est assez probable, logique, que les solutions y ressembleront. » Le responsable projet Inside a noté qu'au niveau des transactions bancaires, « les institutions financières disposent de systèmes de cotations des attaques avancés. » Il a terminé en affirmant : « de toute façon, dans le NFC aujourd'hui, il y a beaucoup de flottement... c'est une technologie non stabilisée. Des expérimentations sont en cours mais il y a beaucoup d'incertitude autour de la certification. »

Comme on peut le constater dans cet extrait, la reconnaissance de cette incertitude sur la standardisation ne constitue pas une raison suffisamment forte pour diminuer *l'enthousiasme technologique* de l'équipe-projet. La possibilité d'échec des processus de standardisation et de normalisation du NFC n'est prise en compte qu'à la condition de s'inscrire dans l'horizon du présent. Or, *l'enthousiasme technologique* permet, à celui qui y souscrit, de dépasser cet horizon. Ce faisant, l'absence de standardisation effective est exclue du champ problématique du projet. C'est une catégorie rendue obsolète par son exclusion dans l'angle mort du projet<sup>243</sup> : le « social ».

Concernant l'adoption et l'appropriation futures de l'usage des téléphones NFC, l'indétermination de celles-ci est mise à mal par la dotation du téléphone NFC de ce que Louis Quéré nomme une « *intériorité* », « *le fait que certains objets soient identifiables, observables, utilisables, analysables, descriptibles comme machine à communiquer, que ce soit pour l'usage ou pour le discours, est de part en part une construction sociale dont il faut rendre compte.* » (Quéré, 1992 p. 32). Pour Quéré, cette intériorité permet de

---

<sup>243</sup> « Because many design representations refer to a future situation, *their designers continuously need to make the articulation to the actual situation*, continuously recreating the context of use or making a closure at a different level, if at all. Their interpretations will easily be more dominant than the actual representation, and users will not easily be able to refer to their own understanding. » (Bodker, 1998 p. 118)

comprendre le caractère relationnel de l'objectivité des machines à communiquer. Une relation qui s'exprime indépendamment de leur fonctionnement opératoire mais qui renvoie aux capacités, aux usages et aux systèmes symboliques qui médiatisent les pratiques.

Ainsi, dans le projet, le téléphone NFC est acté comme lieu d'intégration du CPM à la suite de la **Conférence** téléphonique (T0 + 7) **téléphonique (T0 + 7)** lorsqu'Inside a confirmé qu'il était le dispositif privilégié de diffusion de la technologie. Cette confiance dans le succès de cette association fait écho au travail de persuasion mené par les parties prenantes du développement de cette technologie. La foi des promoteurs dans la diffusion cette technologie provient de ce que ceux-ci considèrent, dans le droit fil du concept d'Intelligence Ambiante, que le téléphone NFC tire sa force de son usage simplifié et instinctif. Les citations suivantes, issues de la littérature spécialisée, illustrent cette vision d'une technologie simple, amenée à être intégrée dans des cercles sociaux hétéroclites et pouvant être assimilée par des usagers novices :

*« Think about the way in which mobile phones have made it so easy to be in touch with people – friends, family, co-workers – from just about anywhere: no cords, no coins, no laborious connections or tedious routines to remember. Then think about what it would be like if other electronic devices in your life worked as easily and as intuitively—if you could set up connections with a simple touch or transfer information from one device to another just by holding them close to one another. This is the promise of Near Field Communication technology – to provide the key to ubiquitous wireless networking of all kinds. It is a powerful catalyst – a highly stable wireless connectivity technology – that provides intuitively simple and safe two-way interactions between electronic devices. It has the potential to make almost all wireless technologies easy enough so that everyone-- even the non-technical-- can use them. »* (NFC forum)

*« NFC makes life easier - it's easier to get information, easier to pay for goods and services, easier to use public transport, and easier to share data between devices. You simply bring NFC-compatible devices close to one another, typically less than four centimeters apart. The benefits of NFC technology are so attractive that many branded service providers are using NFC technology to enhance their services and customer experience. NFC-enabled services are fast and easy to use without compromising existing service security. »* (NFC forum)

*« The fusion of interaction and discovery technologies can facilitate easy, intuitive and impromptu access to networked entities by users without the need for significant administrative overhead. Traditional service discovery methods fail to meet the demands*

*placed by such environments due to mobility, intermittent connectivity, complex configuration and small user interfaces. » (Antoniou & Varadan, 2007)*

*« New technologies, like NFC (Near-Field Communication), might support the independent living of elderly people and improve their quality of life. In this way, it could also be possible to achieve cost savings in the aging society. Meal programs and meals-on-wheels services are very important for elderly people who are not able to cook balanced food for themselves. » (Siira & Haiko, 2007)*

*« Near Field Communication (NFC) allows people to interact with physical spaces and objects by the action of touching a mobile phone to an RFID tag. This is perhaps the first sign of mobile phone being central to the early adoption of the internet of things, where otherwise 'dumb' or 'silent' objects right at the very edges of the network are enabled through the action of touch. » (Arnall, 2006)*

L'équation est alors simple et sa résolution aisée. Puisque le téléphone mobile est déjà un système plébiscité et que le NFC en simplifiera l'usage, le téléphone NFC peut légitimement faire l'objet de projection d'usages par ses promoteurs. Il s'impose comme le cheval de Troie du développement et de la diffusion de la technologie NFC. L'intériorité<sup>244</sup> de cette technologie se déploie par son inscription dans cet environnement à venir et technologiquement enthousiaste<sup>245</sup>. Elle est même supérieure à celle d'autres modes de communication sans fil jusqu'ici articulés avec le téléphone mobile comme le Bluetooth, la 2G, le SMS, la 3G, l'infrarouge (Agnieszka, 2005).

Au sein du projet, cette *pré-dotation en intériorité* est amendée par le manque d'applications en développement :

« Inside précise enfin que “ ce qu'il manque aujourd'hui pour le NFC, ce sont les applications. Aucun fournisseur ne propose encore de services en masse mais il y a quelques exemples pilotes dans les transports. Les opérateurs poussent autant que les fournisseurs de téléphones ”. Le chef de projet complète l'intervention en affirmant qu'à terme, le but est

---

<sup>244</sup> Dans le même article, Quéré précise ce qu'il entend par intériorité : « [...] la possibilité même de s'interroger sur les effets éventuels des NTIC sur le champ social de la communication, sur les formes de la sociabilité ou sur la structure de l'espace public, est créée par une opération antérieure de liaison, qui fait l'objet d'un travail social. Cette opération consiste à doter ces objets d'une « intériorité », c'est-à-dire de capacités d'agir et de réagir, d'affecter et d'être affecté, relatives à des domaines de pratiques socialement organisées. Les pratiques et les « affections » étant articulés par un langage et par des médiations symboliques, ce sont aussi ceux-ci qui sont ainsi incorporés à l'individualité des objets. C'est aussi de cette façon qu'ils acquièrent leur analysabilité et leur descriptibilité dans et pour une communauté de langage et de pratiques. » (Quéré, 1992 p. 36-37)

<sup>245</sup> Cette emphase sur le lien entre simplicité d'utilisation et adoption est tempérée par quelques études ergonomiques (Vassilis & Eamonn, 2007) qui, en réalité, ne remettent pas en cause le lien établi. Le téléphone mobile est ici gage de l'intériorité de cette technologie en développement car c'est un dispositif familier des populations et dont l'utilisation est large.

néanmoins l'interactivité totale entre dispositifs intégrés des tags NFC : ordinateurs, imprimantes, appareils photos. » **Comité de pilotage 2 (T0+3)**

Cependant, en ayant circonscrit la problématisation à la question de la sécurisation de l'information échangée, la question des applications est reléguée au second plan. Elle ne fait pas, non plus, directement partie du problème à résoudre par le faisceau de solutions en présence. Nous allons à présent aborder la manière dont l'équipe-projet s'est emparé de l'élément le plus problématique à *technologiser* : l'utilisateur.

### 3) Les figures de l'utilisateur

La présence de l'utilisateur durant les phases de recherche ou de développement technologique a fait l'objet de nombreux travaux académiques qui en analysent les formes dans la conduite de l'innovation. L'influence de cette présence est telle qu'elle a mené Steve Woolgar à identifier le travail de développement technologique<sup>246</sup> d'un ordinateur de bureau à un travail de configuration de l'utilisateur :

« *The whole history of a system project can be construed as a struggle to configure (that is define, enable and constrain) the user.* » (Woolgar, 1994 p. 207).

On constate ici qu'en réalité, le titre de l'article de Woolgar « *Configuring the user. The case of usability trials* » (1991) véhicule une lecture réductrice du travail de configuration évoqué. Bien que l'auteur ne l'affirme pas explicitement dans le texte, le lieu de la configuration est moins l'utilisateur que la situation d'utilisation tout entière, configurée durant les tests d'« utilisabilité ». Avant de développer notre réflexion à partir de cette première critique, revenons tout d'abord sur la principale critique attachée au texte de Woolgar : l'étendue réduite du lieu d'investigation.

Pouvant paraître relativement déplacée au regard des objectifs de recherche du sociologue britannique, cette critique a toutefois donné lieu au déplacement de la focale d'observation de la configuration de l'utilisation vers d'autres endroits que la conception technologique (Bruce, 1987 ; Boullier, 1994 ; Karat, 1997 ; Green, Harper, Murtagh & Cooper, 2001 ; Bowers & Martin, 2003 ; Oudshoorn, Rommes & Stienstra, 2004 ; Oudshoorn & Pinch, 2005). En sus de la diversification des lieux d'observation, il nous faut également prendre en compte les nombreux travaux qui constituent un plaidoyer pour l'élargissement de champs d'investigation sans pour autant rejeter l'importance de l'étape de

---

<sup>246</sup> Le processus de développement technologique est ici envisagé du point de vue de sa finalité qui consiste en : « defining the identity of putative users, and setting constraints upon their likely future actions. » (Woolgar, 1991 p. 59)



la conception<sup>247</sup>. Ainsi, la technique du prototypage rapide (« *rapid prototyping* ») a tenu lieu d'entrée pour explorer les interactions entre opérations de configuration des concepteurs et usages effectifs de la technologie durant sa phase de développement (Mackay, Carne, Beynon-Davies & Tudhope, 2000). Dans le même ordre d'idée, et avec le succès qu'on lui connaît, l'approche sémiotique ambitionne d'équiper l'analyste d'un vocabulaire performant pour suivre la dynamique de la configuration et de l'usage à travers le cycle de vie de l'innovation technologique (Akrich & Latour, 1992). Cette approche a ceci de particulier qu'elle ne considère pas seulement la dualité usagers/producteurs, mais raisonne en termes d'assemblées d'humains et de non humains formant des équilibres précaires puisque contingents des vicissitudes du projet. Au cœur de cette grammaire de l'action se trouve le concept de « script » et ses déclinaisons :

*« For some time sociologists of technology have argued that when technologists define the characteristics of their objects, they necessarily make hypotheses about the entities that make up the world into which the object is to be inserted. Designers thus define actors with specific tastes, competences, motives, aspirations, political prejudices, and the rest, and they assume that morality, technology, science, and economy will evolve in particular ways. A large part of the work of innovators is that of “inscribing” this vision of (or prediction about) the world in the technical content of the new object. I will call the end product of this work a “script” or a “scenario” ». The technical realization of the innovator's beliefs about the relationship between an object and its surrounding actors is thus an attempt to predetermine the settings that users are asked to imagine for a particular piece of technology and the prescriptions (notices, contracts, advice, etc.) that accompany it. To be sure, it may be that no actors will come forward to play the roles envisaged by the designer. Or users may define quite different roles of their own. If this happens the object remains a chimera, for it is in confrontation between technical objects and their users that the latter are rendered real or unreal. [...] Thus, like a film script, technical objects define a framework of action together with the actors and the space in which they are supposed to act. » (Akrich, 1992 p. 207-208)*

Cette approche sémiotique, en définissant le rôle de chacun des actants agissant dans l'assemblée hétérogène d'humains et de non humains, a le mérite de rééquilibrer la

<sup>247</sup> Patrice Flichy dans (2008) s'étonne que l'on présente Steve Woolgar comme l'initiateur de l'approche sémiologique alors qu'il « semble ignorer l'article de référence de Stuart Hall intitulé justement « Codage, décodage » et qui montre dans le cas de la télévision comment le téléspectateur peut décoder une émission selon un mode différent de celui retenu par le producteur pour l'encodage. Le téléspectateur peut soit ne suivre qu'une partie des inscriptions du message, soit rejeter en bloc le message. Cette autonomie du téléspectateur sera à la base de nombreux travaux sur la réception de la télévision que je présenterai plus loin. De même, les sociologues du travail avaient observé depuis longtemps l'écart important qui existait entre le travail prescrit par la machine ou par l'organisation et le travail réel de l'ouvrier. » (Flichy, 2008 p. 151)

dissymétrie originelle présente chez Woolgar. L'utilisateur, comme l'ensemble des autres actants, est une figure dont on peut vérifier le dynamisme et l'« *agency* »<sup>248</sup> par l'observation des processus de négociations entre les rôles qui lui ont été prescrits et ceux observés dans le fonctionnement dynamique de cette assemblée hétérogène<sup>249</sup>. Ici, l'analyste ne restreint pas la définition de l'utilisateur à celle offerte par les acteurs observés (les concepteurs), une démarche qu'Akrich condamne pour sa coloration technologiquement déterministe<sup>250</sup>.

Ainsi, tandis que Steve Woolgar met l'accent sur la conflictualité présente durant les phases de développement technologique pour configurer l'utilisateur (donc en réalité, l'utilisation) - « *a struggle to configure (that is to define, enable, and constrain) the user* » (Woolgar, 1991 p. 69), son approche pêche en ce qu'elle désincarne au maximum la figure de l'utilisateur. Elle n'en retient qu'une vision « ergonomiste » qui coïncide avec le cadrage des acteurs : l'utilisateur n'est envisagé que comme utilisateur. On comprend, dès lors, que l'analyse ne soit centrée que sur les conflits de configuration de l'interaction homme-machine, l'épaisseur sociale du premier terme étant univoque. En rapatriant l'utilisateur réel dans l'analyse, Madeleine Akrich, n'étend pas seulement le champ d'observation empirique. Elle rétablit l'intérêt d'une prise en compte de l'épaisseur sociale de cet actant particulier qu'est l'utilisateur. Le « *script* », l'« *inscription* » et la « *description* » permettent de saisir la complexité d'un processus d'innovation incomplètement compris comme « *something done to someone* » (Martin, Rooksby & Rouncefield, 2007 p. 302). L'analyse mérite que l'on s'intéresse de près à ce quelque chose, le « *something* » ainsi qu'à ce quelqu'un, le « *someone* », et à la dynamique itérative de définition réciproque de ces deux termes.

Cependant, et malgré la richesse de ses travaux (Akrich, 1989 ; 1992 ; 1993 ; 1995 ; 2001), les analyses de Madeleine Akrich peuvent encourager à négliger la phase de conception technologique comme un lieu d'intérêt analytique pleinement accompli. Si l'entreprise de réconciliation de la sociologie de l'innovation et de la sociologie de l'action

<sup>248</sup> En simplifiant grossièrement cette notion, il s'agit de la capacité d'un acteur à faire des choix et à les imposer à d'autres acteurs.

<sup>249</sup> « To understand the design process of technical artifacts, we should not restrict ourselves to the social groups of design-room engineers or laboratory personnel. Basic to all « new » technology studies is the observation that even in the diffusion stage, the process of innovation continues. » (Bijker, 1992 p. 97)

<sup>250</sup> « [...] it becomes more difficult to uncover the links between technical choices, users' representations, and the actual uses of technologies. Thus the method of content analysis, as applied to texts, adopts an individual and psychological approach that has little or no relevance to our problem. Indeed, because it ignores the wide range of uses to which objects may be put, it comes close to technological determinism. [...] One way of approaching the problem is to follow the negotiations between the innovator and potential users and to study the way in which the results of such negotiations are translated into technological form. Indeed, this method has been widely used in sociological and historical studies of technology. [...] Instead we have to go back and forth continually between the designer and the user, between the designer's projected user and the real user, between *the world inscribed in the object* and *the world described by its displacement*. » (Akrich, 1992 p. 208-209)

commande de s'intéresser à l'utilisateur réel<sup>251</sup> (Akrich, 1993), nous pensons que les disputes qui animent le processus de configuration de l'usage demeurent des moments d'étude à part entière pour l'approfondissement du savoir sur la co-construction des technologies et de leurs utilisateurs, notamment lorsqu'il s'agit de processus d'innovations exploratoires (Dubey & Moricot, 2006 ; Stewart & Claeys, 2009). Il appartient alors à l'analyste de poser un regard acéré sur les différentes manières qu'ont les projets de rendre présent l'utilisateur, figure charnière d'un processus de configuration plus large, la *projection d'usages*.

En nous intéressant à la mise au monde de l'utilisateur dans la *projection d'usage*, nous souhaitons rendre compte du processus de mise en conformité qui autorise l'articulation d'une figure de l'utilisateur à *l'enthousiasme technologique* de la projection. Soumis à une grille de lecture « technologique », l'utilisateur est *technologisé* pour être mieux mobilisé. Il est contraint à l'adoption d'une posture conforme au projet, celle de l'utilisateur, tandis que les autres postures, pourtant nombreuses, sont reléguées à l'arrière-plan.

### **Les différentes postures<sup>252</sup> de l'utilisateur : l'utilisateur comme posture contrainte**

Nous avons identifiés neuf postures de l'utilisateur maniées par l'équipe-projet

- le citoyen
- le client
- l'utilisateur
- les institutions émettrices de normes prescriptives
- les institutions économiques
- les institutions représentatives de l'utilisateur
- le peuple
- le marché
- et enfin les utilisateurs.

---

<sup>251</sup> De nombreux travaux plaident pour l'extension de la sphère de compréhension de l'utilisateur à d'autres postures que celles d'utilisateur, au sens ergonomique du terme (Kline & Pinch, 1996 ; van Kammen, 1999 ; Epstein, 2003 ; Oudshoorn & Pinch, 2003 ; van Kammen, 2003 ; Oudshoorn & Pinch, 2005 ; Martin, Rooksby & Rouncefield, 2007)

<sup>252</sup> Pour Madeleine Akrich, la posture « désigne l'acteur pris dans une relation ou un ensemble de relations régies par un unique principe d'équivalence : l'abonné, le spectateur, le contribuable sont autant de termes spécifiant une posture qui peut être assignée à l'usage des réseaux. Chaque posture est associée à un ensemble de dispositifs techniques et sociétaux. » (Akrich, 1993 p. 48)

L'analyse montre que ces postures ne sont pas exclusives. Elles résultent de deux facteurs de compréhension de l'utilisateur. D'un côté, celui-ci est intégré comme partie d'une écologie sociotechnique plus ou moins étendue. La largeur de l'écologie sociotechnique balaye ainsi un espace qui part *a minima* du dispositif technologique (le CPM) jusqu'à une plus large prise en compte des rapports avec d'autres dispositifs de toutes sortes (technologiques, juridiques, géographiques, politiques, organisationnels, sociaux, etc.). De l'autre côté, l'humain est appréhendé selon différents niveaux de granularité : de l'unité élémentaire à la masse d'individus. A la croisée de ces deux facteurs, nous avons identifié trois *champs d'action* et trois *modes d'existence* à l'intérieur desquels se dégagent les différentes postures autorisées de l'utilisateur<sup>253</sup> dans le projet.

Les trois *champs d'action* identifiés sont le *politique*, l'*économique* et l'*ergonomique* (voir Figure 37. Les champs d'action de l'utilisateur) ci-dessous. Chacun de ces champs est constitué par trois postures.

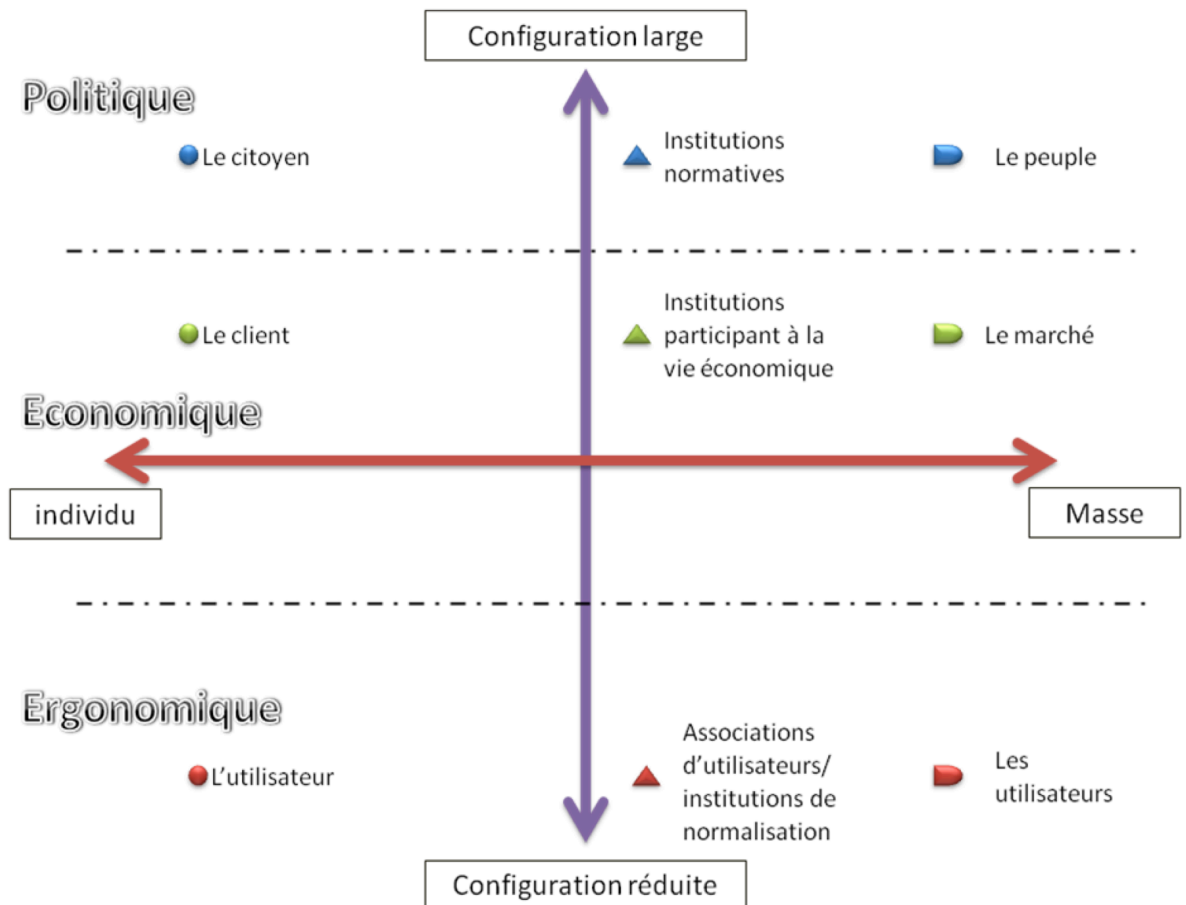
Dans le champ politique, il s'agit du *citoyen*, de toute *institution détentrice d'un pouvoir normatif* et enfin du *peuple*. Dans ce champ, l'utilisateur est défini dans ses relations à l'« espace public » (Habermas & Quéré, 1989), espace ici structuré par un ordre juridique<sup>254</sup>. Le champ économique est peuplé de la posture du *client*, de toute *institution participant à la vie économique* (économie sociale comprise) et du *marché* régissant cette vie économique. Ici, l'activité humaine implique la production, la distribution, l'échange et/ou la consommation de biens et services. Le marché, comme espace de rencontre entre offre et demande, est ici considéré comme un acteur plutôt que comme un espace exogène structurant.

Enfin, dans le champ ergonomique, il y a la posture de l'*utilisateur*, la posture de toute *institution représentative de certaines classes d'utilisateurs* et enfin la *masse d'utilisateurs*. Ce dernier champ marque l'action de l'utilisateur dans sa confrontation directe et matérielle au dispositif technologique. Lors de la réunion de lancement, l'utilisateur, qui était quasi unanimement désigné comme « l'utilisateur », fut évoqué à travers l'ensemble des trois champs d'action.

<sup>253</sup> Les champs d'action et les modes d'existence identifiés empiriquement ont vu leur analyse largement inspirées par la déconstruction de l'utilisateur en quatre états établie par Dominique Boullier : « Il est récepteur lorsque dans le message, il traite une représentation à travers la médiation du langage ; il est utilisateur (ou exploitant) lorsque, dans l'ouvrage, il traite son activité à travers la médiation de la technique ; il est usager (au sens strict cette fois) lorsque dans l'usage, il traite son appartenance à travers la médiation de la société ; il est consommateur ou électeur, lorsque dans le suffrage, il traite son désir à travers la médiation de la norme. » (Boullier, 1994).

<sup>254</sup> « Relativement à une entité (Etat, groupe d'Etats, etc., l'ensemble des règles de Droit qui la gouvernent. Ex. l'ordre juridique français, international, mais aussi d'après les conceptions de l'institutionnalisme italien (Santi Romano), l'ordre juridique de l'Eglise, d'une commune, d'une entreprise. » (Cornu, 1987 p. 601)

Figure 37. Les champs d'action de l'utilisateur



La description de ces champs d'action est, en creux, celle de ce que nous avons nommé des *modes d'existence* qui, comme les précédents, se déclinent en un trio (voir figure 38). Il s'agit du mode *atomique* dont l'utilisateur, le client et le citoyen font partie ; du mode *public* dont font partie les *corporations* que sont les institutions normatives, économiques ou de représentation des utilisateurs ; et enfin du mode de la *foule*. Les deux derniers modes d'existence sont librement inspirés de la catégorisation établie par Gabriel Tarde distinguant le « *public* » de la « *foule* ».

Le *public* désigne l'ensemble des entrepreneurs qui jouent, légitimement ou non, le rôle de porte-parole de la *foule*, ce que Pierre Chambat nomme la « *captation de la représentation*<sup>255</sup> » de groupes latents<sup>256</sup>. Ainsi, le *public* est envisagé ici en rapport à sa

<sup>255</sup> « L'expression d'intérêts, des représentations ou des demandes de ces groupes latents est généralement assurée par des « entrepreneurs » extérieurs, des acteurs qui se présentent comme leur porte-parole. » (Chambat, 1994 p. 48). L'auteur explique ce constat par le fait que « (...) l'atomisation des utilisateurs, leur faible degré d'organisation et l'institutionnalisation très limitée des scènes où leur pont de vue peut être exprimé et rendu visible, les rapproche d'une situation de marché où l'expression des préférences s'exprime par la décision d'achat d'un bien. » (Chambat, 1994 p. 48)

superposition aux groupes institués<sup>257</sup> tandis que c'est le trait incontrôlable, multiforme et dangereux de la *foule* que nous souhaitons souligner<sup>258</sup>. Aussi, les liens qui animent les relations entre ces deux termes<sup>259</sup> ont trouvé écho dans les discours des partenaires au projet lors de la réunion de lancement. Ainsi, le CEA-LETI a lancé une distinction visant à distinguer chez l'utilisateur les « peurs irréelles » des « peurs fondées », le critère de validité du fondement étant la possibilité technique d'avènement d'un événement au fondement de la peur.

Cette distinction constitue la base d'une catégorisation de la cible à adresser prioritairement dans le projet : c'est sur le champ d'action *ergonomique* et sur les manières d'être *atomiques* que le travail se concentre. Les autres champs, en raison de l'ambition relative du projet et du faisceau de solutions en présence, sont relégués à la périphérie du projet : le champ d'action *économique* et le champ d'action *politique* s'ils sont évoqués, ne font l'objet de discussions approfondies que lorsqu'ils entrent en conjonction avec la manière d'être *atomique* (cf. **Réunion interne (T0 + 10)** et **Conférence téléphonique (T0 + 15)**). A titre d'exemple, lorsque l'entreprise Inside a fait état de l'absence de modèle économique (« business model ») existant pour l'intégration de la technologie NFC au téléphone portable, aucune partie au projet n'a semblé s'en inquiéter plus que de rigueur (cf. **Comité de pilotage 1 (T0)**). Une autre illustration est la définition des scénarios par le CEA-LETI comme un ensemble de « menaces, de moyens à mettre en œuvre pour attaquer la « Privacy » de l'utilisateur et le coût envisagé de la protection à mettre en place ». Ces trois critères fondaient alors la pertinence du choix des scénarios à effectuer pour engager le travail de spécification des fonctions de la preuve de concept. En réalité, cette attention

---

<sup>256</sup> Il affirme que l'ensemble formé par les usagers est « composé d'individus, de ménages, atomisés pour lesquels les caractéristiques communes ne suffisent pas à déboucher sur une identité d'intérêts ni, *a fortiori*, sur une action collective se traduisant par la formulation de leurs intérêts. En d'autres termes les usagers constituent un « groupe latent. » (Chambat, 1994 p. 47)

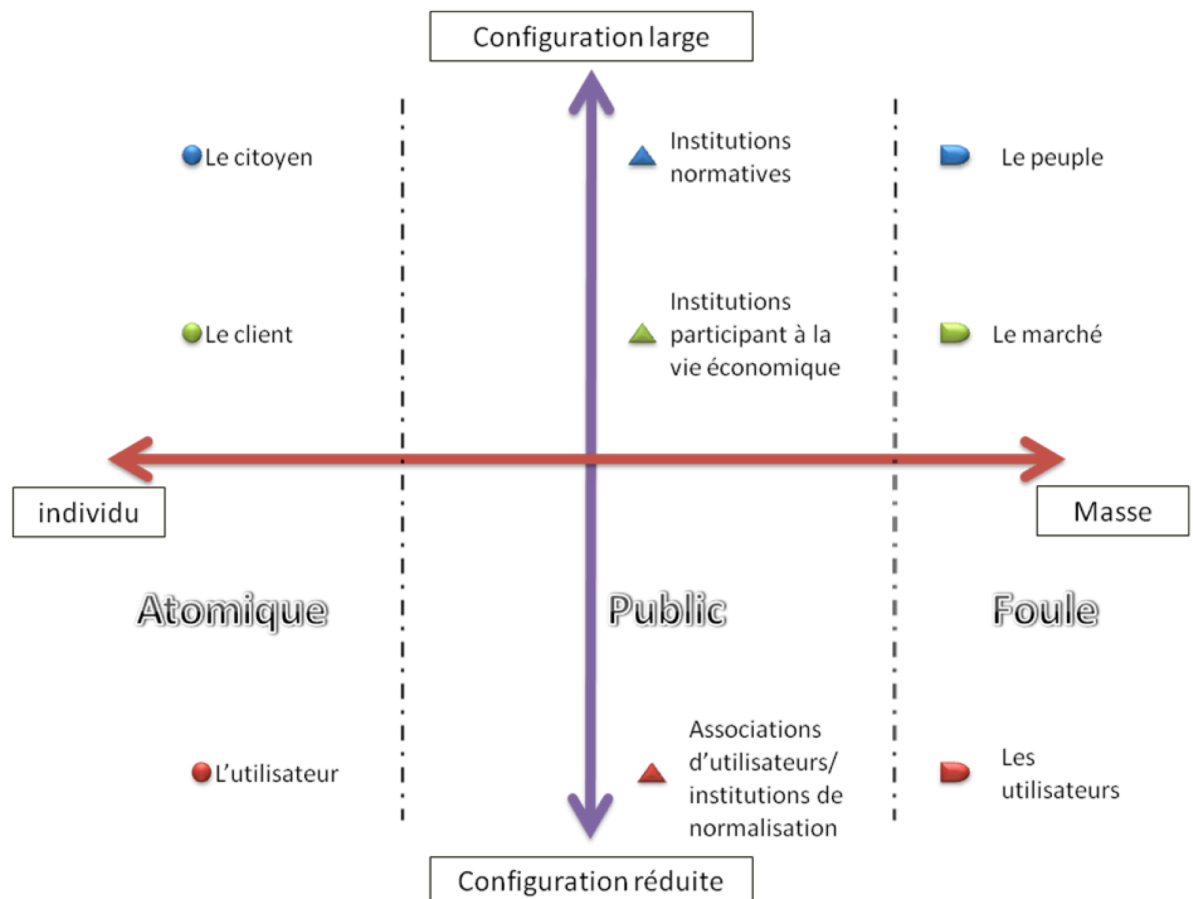
<sup>257</sup> « Or, il suffit d'ouvrir les yeux pour s'apercevoir que la division d'une société en publics, division toute psychologique, et qui correspond à des différences d'états d'esprit, tend, non pas à se substituer sans doute, mais à se superposer de plus en plus visiblement et efficacement à sa division religieuse, économique, esthétique, politique, en corporations, en sectes en métiers, en écoles, ou bien en partis. Ce ne sont pas uniquement ces variétés des foules d'autrefois, les auditoires des tribuns ou des prédicateurs, qui sont dominés ou agrandis par les publics qui leur correspondent, public parlementaire ou public religieux; mais il n'est pas une secte qui ne veuille avoir son journal à soi pour s'entourer d'un public qui rayonne bien au-delà d'elle, sorte d'atmosphère ambiante où elle sera baignée, de conscience collective dont elle sera illuminée. » (Tarde, 1901 p. 17-18).

<sup>258</sup> « Mais, si diverses qu'elles soient par leur origine, comme par tous leurs autres caractères, les foules se ressemblent toutes par certains traits : leur intolérance prodigieuse, leur orgueil grotesque, leur susceptibilité née de l'illusion de leur toute puissance, et la perte totale du sentiment mutuellement exaltées. Entre l'exécration et l'adoration, entre l'horreur et l'enthousiasme, entre les cris *vive* et *à mort*, il n'y a pas de milieu pour une foule. *Vive*, cela signifie *vive à jamais*. Il y a là un souhait d'immortalité divine, un commencement d'apothéose. Il suffit d'un rien pour changer la divinisation en damnation éternelle. » (Tarde, 1901 p. 22)

<sup>259</sup> « Combien tout cela nous éloigne des crimes du public ! Le public, quand il est criminel, l'est par intérêt de parti plus que par vengeance, par lâcheté plus que par cruauté ; il est terroriste par peur, non par accès de colère. Il est capable surtout de complaisance criminelle envers ses chefs, de *manutengolisme*, comme disent les Italiens [...] Quant au public même, il reste dans l'ombre, insaisissable, attendant l'heure de recommencer. Le plus souvent, quand une foule commet des crimes, - à commencer par les parlements, foules à demi corporatives, qui se sont montrés les complices de tant de despotes, - il y a derrière elle un public qui la meut. » (Tarde, 1901 p. 32)

particulière attribuée au *champ d'action ergonomique* et à la *manière d'être atomique*, n'évince pas seulement les autres figures de l'utilisateur convoquées au projet, elles bâillonnent aussi leur expression pour qu'ils n'entravent pas le processus de stabilisation de l'écologie socio-technique en élaboration. Une fois celle-ci stabilisée, les usagers seront convoqués par un autre biais (les entretiens individuels faisant office d'étude d'acceptabilité) pour consolider la projection d'usage.

Figure 38. Les modes d'existence de l'utilisateur



Cette considération est acte de validation tacite d'un porte-parole privilégié de l'identité de l'utilisateur : les *données*, soit des « descriptions élémentaires, souvent codées, d'une chose, d'une transaction d'affaire, d'un événement, etc. » (définition de la donnée informatique selon Wikipedia<sup>260</sup>). La consécration des données comme porte-parole légitime désignent les usagers, dès le départ du projet, comme des quasi « *Cyborgs* »<sup>261</sup>. Les données

<sup>260</sup> [http://fr.wikipedia.org/wiki/Donn%C3%A9e\\_\(informatique\)](http://fr.wikipedia.org/wiki/Donn%C3%A9e_(informatique))

<sup>261</sup> « A Cyborg is a cybernetic organism, a hybrid of machine and organism, a creature of social reality as well as a creature of fiction. Social reality is lived social relations, our most important political construction, a world-changing fiction. [...] The Cyborg is resolutely committed to partiality, irony, intimacy, and perversity. It is oppositional, utopian, and

inscrivent l'utilisateur et son action dans, hors et à travers le dispositif technologique. La récurrence de l'utilisateur comme amas ou flux de données est la version exacerbée de la désincarnation sociale de la figure de l'utilisateur par les acteurs du projet. En fin de réunion (**Réunion téléphonique (T0 + 10)**), le CEA-LETI a effectué un rappel des objectifs du projet en ces termes : « introduire dans le scénario des aspects très liés aux données personnelles, comme la fuite de données figurant dans des agendas, des photos, des emails, des choses comme ça ! ».

Plus loin, en considérant comme seules variables de distinction de ces différentes postures la granularité et l'« *agency* » de l'utilisateur, les membres du projet en appréhendent la multiplicité tout en en réduisant drastiquement l'épaisseur sociale. L'une des conséquences de cette appréhension réductrice est la pétrification de l'utilisateur dans une posture unique : en sus d'être dépourvu de genre, de préférences, de professions, d'appartenances multiples<sup>262</sup>, l'utilisateur est une entité figée aux compétences données et stables. Cela implique notamment l'ignorance possible, par l'équipe-projet, des possibilités d'apprentissage (von Hippel & Tyre, 1995) à l'œuvre lors de l'appropriation d'un dispositif technique. Pire, en niant l'apprentissage dans l'usage projeté, l'on peut supposer que l'apprentissage dans la conception soit entravé par la dénégation de l'utilisateur comme possible source d'innovation (Rosenberg, 1976 ; von Hippel, 1976 ; David, 1986 ; Andersen & Lundvall, 1988 ; Habermeier, 1990 ; Slaughter, 1993 ; Fleck, 1994). La planification d'une étude d'acceptabilité en fin de course du projet témoigne de ce déni.

En somme, l'utilisateur est passif. Sa mise en données permet de faire primer ses qualités d'agent sur ses capacités d'acteur. Cette substitution de l'être à l'agir rend possible l'intéressement de l'utilisateur à la dynamique de conception et à la gestion par projet : il devient une figure univoque, malléable et appréhendable par les autres acteurs. Donner vie à l'utilisateur consiste donc à le contraindre à l'adoption d'une posture d'utilisateur pour qu'il puisse exister dans le script construit. Alors, il est agi par la configuration sociotechnique qui réagit à ses comportements ergonomiques. Il est à la fois compris comme isolé dans

---

completely without innocence. No longer structured by the polarity of public and private, the Cyborg defines a technological polls based partly on a revolution of social relations in the oikos, the household. Nature and culture are reworked; the one can no longer be the resource for appropriation or incorporation by the other. The relationships for forming wholes from parts, including those of polarity and hierarchical domination, are at issue in the Cyborg world.» (Haraway, 1991 p. 149-151)

<sup>262</sup> « Users are simultaneously consumers, citizens, members of a family, of a religious faith, of a social club, of a political party, of a profession, or whatever. In many cases, technical design debates turn on the need to arbitrate between varying positions of the user which are more or less incompatible within a single technological system. Accordingly creating a market invariably means tuning in to several wavelengths simultaneously. The way an innovation takes hold cannot be reduced to any one model, e.g. the rational economic consumer, the status-seeking purchaser or the inveterate trend-follower. Instead, the success or failure of innovations frequently depends on their ability to cope with dissimilar users possessing widely differing skills and aspirations. » (Akrich, 1995 p. 167)



l'action et numérisable à l'intérieur de l'action. L'extrait suivant est particulièrement significatif de ce travail de réduction des contraintes visant à stabiliser l'utilisateur<sup>263</sup> dans le projet :

« Durant plusieurs réunions, nous avons discuté de la manière d'évaluer les menaces qui pèsent sur la « *Privacy* » d'un dispositif, le CPM, dont le fonctionnement nous échappe encore dans sa globalité. Par ailleurs, les conclusions que nous avons tirées dans l'état de l'art nous compliquaient la tâche : la notion de « *Privacy* » se révélait être une notion complexe, protéiforme et fortement dépendante tant des contextes d'utilisations que de la perception de l'utilisateur. Cependant, ce travail a permis la découverte de plusieurs pans de littérature spécialisée dans l'électronique et les interactions homme-machine caractérisés par une volonté d'opérationnalisation des recherches. Ainsi, pour apporter notre pierre à l'évaluation des scénarios, nous avons intégré une grille d'analyse empruntée au HCI qui permettait, *a minima*, de rendre l'utilisateur potentiel présent durant la conception. Les deux variables clés constituant cette grille étaient celles du « contrôle » et du « feedback » offerts à l'utilisateur et nous permettaient de visualiser sur un même plan les différences entre options techniques en termes d'implication de l'utilisateur dans l'usage du CPM. Ainsi, les trois options techniques figurant dans le scénario « Payment » élaboré par Inside et UVSQ ont été intégrées dans la démarche d'évaluation après que nous nous soyons acharnés à les comprendre, sans être pour autant certains d'y être parvenu. Ce faisant, en prenant en compte la manière dont ces options pourraient être perçues par l'utilisateur, nous avons découpé l'une d'elles en deux possibilités d'usages. Au total, nous obtenions donc quatre « options d'usage » pour trois options techniques. En deuxième lieu, nous avons choisi d'élaborer des hypothèses à partir de cette première analyse en nous basant sur le travail effectué durant la revue de littérature sur la notion de confiance. Il s'agissait pour nous de comprendre sur quelle entité l'utilisateur devait se reposer et, conséquemment, vers qui il pourrait se retourner en cas d'échec de la protection. » **Réunions internes (T0 +15)**

Cette réduction de l'utilisateur à un utilisateur traduit en données numériques ne résout cependant pas la question de la représentation de l'utilisateur durant cette phase du projet pendant laquelle les données sont tout à la fois muettes et projetées. En effet, nous devons

---

<sup>263</sup> « Le client? Quand on l'invoque on croit tenir un être concret alors qu'il s'agit de l'abstraction la plus forte qui soit ! Il est multiple, évanescent, il tient plusieurs discours et vous lâche au moment même où vous pensiez le tenir. Au lieu d'un seul représentant ou d'un seul porte-parole, vous êtes confronté à plusieurs intermédiaires qui prétendent vous dire ce que veulent les utilisateurs. Si le client était clairement identifiable, prévisible, loyal et s'il savait toujours ce qu'il veut vraiment, alors l'innovation serait une véritable partie de plaisir. Pour se développer, il lui faut souvent cet espace incertain, ces mouvements inattendus qui rendent évanescents des marchés qui semblaient pouvoir durer et laissent entrevoir des réorganisations bénéfiques. Le client est roi, mais d'un empire dont les frontières sont mal définies et dont les lois sont floues. C'est un être énigmatique. C'est pourquoi les études de marché ou les contacts avec les utilisateurs ressemblent parfois à des traques nécessaires mais désespérées. Les agents doubles sont partout et difficiles à démasquer. L'innovation ressemble plus aux romans de John le Carré qu'à ceux d'Agatha Christie. » (Akrich, Callon & Latour, 1991 p. 45)

aborder la question de la mise en présence de l'utilisateur dans cette partie du projet en répondant à la question de l'expression de ces données : qui parle pour l'utilisateur dans le projet ?

### La question de la représentation de l'utilisateur

Dans un chapitre d'ouvrage plaider pour une approche socio-politique des usages<sup>264</sup> (Vitalis, 1994), Pierre Chambat juge la figure de l'utilisateur de TIC « *simultanément centrale et difficilement représentable* » (Chambat, 1994 p. 58). Ce constat fait bien entendu écho aux figures de l'utilisateur qui jalonnent le parcours de vie des TIC, mais il traduit incidemment la diversité des modalités de re-présentation de celui-ci. Dans le cadre de projets de conception technologique exploratoire, l'utilisateur à représenter n'est pas l'unique protagoniste (Schot & Albert de la Bruheze, 2003) : tandis que l'utilisateur réel est alors inexistant et que la notion de « *script* » rend vie à un utilisateur projeté objet d'articulations et de négociations, une troisième figure d'utilisateur complète le tableau, celle de l'utilisateur représenté<sup>265</sup> : « *In the mediation process a number of users proliferate : projected users, real users, and represented users. Implicated in the process of mediation is the contestation of these users and their demands, the quality of projections (by designers), the legitimacy of the representations and the representers, and the acceptance of real users* » (Schot & Albert de la Bruheze, 2003 p. 235).

Deux voies s'ouvrent aux concepteurs pour représenter l'utilisateur : il est soit représenté de manière instituée ou par le biais de l'expérimentation<sup>266</sup>. A celles-ci s'ajoutent de multiples techniques, explicites<sup>267</sup> ou implicites<sup>268</sup> (Akrich, 1995). Parmi les techniques

---

<sup>264</sup> « Une socio-politique des usages ne constitue pas à proprement parler un programme de recherche nouveau, ou une rupture de paradigme, mais une tentative pour articuler dans un même cadre d'analyse les apports respectifs de perspectives existantes qui, chacune, ont mis l'accent sur une dimension particulière de l'usage des technologies. Cette approche consiste à considérer que l'utilisation des technologies dans une société se situe au croisement de quatre logiques. D'une part, une logique technique et une logique sociale qu'il est possible d'articuler en recourant au concept de configuration socio-technique. D'autre part, une logique d'offre et une logique d'usage dont l'interaction complexe peut notamment - mais non exclusivement - être approchée par une analyse en termes de représentation. En croisant ces quatre logiques, il est possible de spécifier les rapports d'usage spécifiques à un système technologique donné, ces rapports d'usage définissant à la fois un rapport à l'objet technique et un rapport social entre les différents acteurs. » (Vedel, 1994 p. 28)

<sup>265</sup> L'étude de la construction d'un scénario renvoie ainsi à la fois à l'étude de l'utilisateur représenté et à celle de l'utilisateur projeté.

<sup>266</sup> « Il s'agit là de deux processus interdépendants de construction de l'utilisateur qui se déroulent sur des scènes multiples, de la littérature spécialisée dans les NTIC aux hémicycles des assemblées parlementaires en passant par les couloirs feutrés des instances de normalisation, voire les laboratoires de recherche en sociologie. Explorer ce que peut recouvrir la notion de représentation des usagers amène donc à dénouer les fils entremêlés de trois questions ou de trois niveaux d'analyse : le statut de la technique, et plus particulièrement des techniques de communication, le statut du quotidien, c'est-à-dire des pratiques de communication dans la construction des modes de vie et de l'être ensemble, et enfin le statut des objets, des machines à communiquer en tant qu'elles sont « une pétrification de rapports sociaux. Mais affronter ces questions conduit à faire exploser la notion d'utilisateur en mettant en évidence les différentes figures qui la composent, les acteurs qui participent à leur construction et les modèles (politique ou économique) qui les sous-tendent. » (Chambat, 1994 p. 59)

<sup>267</sup> « based on special skills or qualifications in the area of defining or interpreting consumer representations. » (Akrich, 1995 p. 169).

explicites figurent les études de marché, les tests consommateurs ou encore les retours d'expérience. Pour les techniques implicites, Akrich relève, sans prétention d'exhaustivité, le recours aux experts, le « *benchmarking* » et enfin la « *I methodology* » qui consiste à attribuer à l'ensemble ou à une partie de l'équipe de conception la légitimité de représentation de l'utilisateur.

C'est cette technique qui est mobilisée dans l'élaboration de la projection d'usage du projet COPRIM. Il est organisé de telle sorte que la problématique de l'extension de l'expertise<sup>269</sup> est réglée par sa stratification dans le projet (cf. Chapitre XIII) : l'utilisateur est un acteur impliqué dans le projet (Clarke, Adele & Montini, 1993) par la présence de deux équipes expertes, Umanlab et l'entreprise INSIDE, toutes deux parlant en son nom<sup>270</sup>. Cette mission s'exprime différemment pour les deux équipes. Elle est explicitement inscrite dans l'annexe technique du projet pour l'équipe Umanlab dont le positionnement d'expert en sociologie des usages est affirmé :

*« Since 1996 this team has been developing and applying the CAUTIC method (Design assisted by the use for technologies, innovation and change) which is used to design new applications and innovative services by considering the user at the most early stage in the process of development. »* (Annexe technique au projet, p. 19)

En ce qui concerne le rôle de représentation de l'entreprise Inside, celui-ci n'est pas directement exposé dans le texte de l'annexe technique. Inside n'y est décrite qu'en qualité d'expert d'un marché en constitution, le NFC, et comme participant actif à sa structuration. En revanche, durant la réunion de lancement du projet, le CEA-LETI, chef de projet, a confié à Inside un mandat de représentation de l'utilisateur par « l'apport de scénarios sur lesquels les clients ont des réticences ou des inquiétudes » (**Comité de pilotage 1 (T0)**). En réalité, en évoquant les clients, le chef de projet faisait référence soit au positionnement des industriels qui constituent la clientèle d'Inside, soit aux utilisateurs putatifs du CPM, futurs clients captifs de ces industriels. Or, finalement, le rôle d'Inside dans la représentation de l'utilisateur a essentiellement consisté à lui donner voix à travers la circulation des données. En

---

<sup>268</sup> « which rely on statements made on behalf of the users. » (Akrich, 1995 p. 169)

<sup>269</sup> « Greater involvement of the public has, however, given rise to the « Problem of Extension » : how do we know how, when, and why, to limit participation in technological decision-making so that the boundary between the knowledge of the expert and that of the layperson does not disappear ? » (Collins & Evans, 2007 p. 19)

<sup>270</sup> « There can also be *implicated actors* in a social world and/or arena, actors silences or only discursively present – constructed by others for their own purposes (Clarke & Montini 1993). This concept provides a means of analyzing the situatedness of less powerful actors and the consequences of others' actions for them and raises issues of discursive constructions of actors and of nonhuman actants. [...] There are at least two kinds of implicated actors. First are those implicated actors who are physically present but are generally silenced/ignored/invisibles by those in power in the social world or arena. Second are those implicated actors *not* physically present in a given social world but solely discursively constructed; they are conceived, represented, and perhaps targeted by the work of those others; hence they are discursively present. » (Clarke, Adele, 2005 p. 46)

ce sens, Inside s'est conformé à l'orthodoxie du projet en ne laissant s'exprimer, dans la projection d'usage, que l'utilisateur.

Les politiques de représentations de l'usager affichées dans l'annexe technique s'inscrivent dans la logique de stratification de l'expertise (cf. chapitre XIII) en attribuant à chaque acteur un domaine réservé relatif à sa position experte. Cependant, tandis que la notion de client permet d'envisager le champ d'action économique comme domaine réservé d'Inside, celle d'usager, « *user* », laisse planer un flou quant au domaine réservé de Umanlab. En analysant le contrepoint que constitue la désignation de représentants de l'usager au sein du projet, nous souhaitons souligner l'élasticité de ces mandats.

Dans un article sur le développement des vaccins anti-fertilité, Jessika van Kammen explore les relations entre groupes de défense d'utilisateurs potentiels et actuels d'une part, et scientifiques d'autre part pour la définition des vaccins (van Kammen, 2003). Elle démontre que ces groupes – notamment des groupes féministes – ont pu bénéficier d'un climat international favorable pour intégrer le programme de réflexion mené par l'organisation mondiale de la santé (OMS). L'auteur constate que cette intégration des « *users' perspectives* » a été accueillie avec enthousiasme par les scientifiques (sciences dures et sciences sociales) et par les représentants politiques habitués à travailler ensemble. Cependant, elle observe que cette initiative a eu pour conséquence un déplacement substantiel du rôle alloué au départ à ces groupes féministes lors de la mise en action du projet :

« [...] to the women's health advocates, “integration of users' perspectives” was the Trojan horse by which they gain access to reproductive and social scientists at WHO/HRP [Human Reproduction Programme of the World Health Organization]. [...] This understanding went beyond the question of what kinds of contraceptive products users want and meant taking into account the users in their contexts, including women's health and their rights, and recognizing the perspectives of women's health groups as valid. » (van Kammen, 2003 p. 160)

Le projet a finalement donné naissance à ce que l'auteur nomme un « *monstre technologique* » intégrant un maximum de représentations des usagers mais incapable d'en attirer aucun, la multiplicité des représentations prises en compte s'étant révélée comme une contrainte pour la conception d'un nouveau contraceptif et a joué un rôle déterminant dans le glissement de mission des groupes féministes. Ceux-ci ont progressivement adopté une

stratégie privilégiant la montée en expertise sur les problématiques scientifiques liées au contraceptif comme moyen de légitimation de leur rôle dans le projet. Ils ont ainsi délaissé l'ambition originale de parler au nom des usagers pour se faire entendre en tant que représentants légitimes de ceux-ci. Cet exemple peut paraître éloigné de notre problématique mais il permet d'en éclaircir plusieurs points.

Intéressons-nous tout d'abord au fait que le rôle de représentation échu à l'équipe Umanlab a été menacé par un travail concurrent de légitimation de leur présence. En effet, la non-familiarité des équipes technologiques avec le travail des sociologues praticiens fait écho à la situation exceptionnelle d'intégration de groupes féministes à une assemblée d'experts hétérogène habitués à travailler ensemble : le groupe d'experts de l'OMS. Similairement aux groupes féministes, les sociologues vont peu à peu passer autant sinon plus de temps à consolider leur position d'expert de l'utilisateur au détriment d'un travail de représentation d'un usager compris dans la diversité de ces postures. Ainsi, tandis que la présence de plusieurs postures de l'utilisateur est résolue par la prise en compte d'une seule de celles-ci, la présence de plusieurs représentants pour une posture unique s'est révélée être un facteur de perturbation de la distribution, non des rôles de représentation, mais des objets de celle-ci.

Dès lors, l'idée de « *monstruosité technologique* », qui désigne, sous la plume de Van Kammen, l'incorporation dans une technologie d'intérêts multiples et divergents, a été évitée par la réduction au silence d'autres postures de l'utilisateur que celle de l'utilisateur. L'ensemble du projet a adopté une « *définition de la situation* » de représentation qui adopte un cadrage univoque (Collins & Pinch, 1982 ; Bijker, 1987 ; Carlson, 1992 ; Flichy, 2003) construit à partir de l'image que les concepteurs se font du monde<sup>271&272</sup>.

---

<sup>271</sup> Voir (Carlson, 1992) et la notion de « cultural creep ». L'auteur explique l'échec d'Edison à promouvoir le kinétoscope par l'inadaptation de son cadre cognitif à un environnement en mouvement. En considérant que le kinétoscope se diffuserait de la même manière que le phonographe, Edison a négligé les attentes d'un public désireux de nouvelles sensations. Il a négligé le travail sur les scénarios ou sur le jeu d'acteurs et à laisser dériver les cadres cognitifs de son équipe dans la conception et la promotion du phonographe. De la même manière, Bardini et Horvath ont créé le concept d'utilisateur réflexif (reflexive user) pour désigner l'identité entre les premiers utilisateurs du PC et les innovateurs de Xerox PARC et de Stanford dans les années 70. Ils ont montré comment leur utilisation précoce de cet instrument avait influé sur les choix techniques effectués par la suite ou encore (Bardini & Horvath, 1995).

<sup>272</sup> A l'avenant, l'on peut légitimement s'interroger sur les liens entre pratiques de représentation (parler pour), effets de cadrage et pratique de conception comme le prône Epstein dans son étude sur les différentes stratégies de représentations d'association de femmes, de politiciennes, de scientifiques, de cliniciens, de représentants de l'industrie pharmaceutique pour représenter l'utilisateur durant l'examen de réformes de politiques publiques de santé : « In some cases, it may be meaningful to speak of the processes by which politically disenfranchised political actors, acting in their own name, directly take up the task of transforming science « from below ». More frequently, I suspect, it may be more accurate and more fruitful to consider the complex practices of representation by which some individuals or entities, located within heterogeneous coalitions, invoke, and speak on behalf of, broader social collectivities. » (Epstein, 2003 p. 189)

Enfin, bien que cela tienne de l'évidence, le caractère exploratoire du projet dans lequel prend part la projection d'usages rend caduque la question de l'arbitrage entre le recours à des représentants des usagers ou celui, plus direct, aux usagers eux-mêmes. Ce problème, qui a fait l'objet de nombreuses analyses des spécialistes de la conception participative (Bloomberg, 1993 ; Grudin, 1993 ; Webb, 1996 ; Axtell, Waterson & Clegg, 1997 ; Kensinger & Bloomberg, 1998 ; Button, Graham, 2000 ; Sanders, 2002) ne peut se poser dans les mêmes termes puisque l'utilisateur, pour être présent doit *être projeté*.

Quant à la notion de « *public*<sup>273</sup> », que John Dewey attachait à celle de problème (Dewey, 1927 ; Brugidou, 2008), celui-ci existe alors en fonction de sa contingence et de sa proximité à un problème qui fonde ses conditions d'origine<sup>274</sup>. C'est une construction qui émerge à travers et autour de problème par le biais de l'action. Dès lors, l'une des questions essentielles devient non pas la formulation du problème pertinent *per se* mais l'articulation de ce problème à l'action de publics potentiels :

*« For Dewey, the problem of the public was not a problem of definition—it was a problem of action. The question of what constitutes a public served to highlight the concern of how a public is—or is not—constituted. The challenge of public action is traced to the inability of a public to form: before a public acts, it must come into being. This inability to form, or form effectively, is not because of a lack of issues, but rather because the issues resist identification and articulation, leaving publics unformed and tentative. »* (DiSalvo, 2009 p. 51)

Cette existence liée du « *public* » et du « *problème* » rend particulièrement sensibles les modalités de figuration et de représentation de l'utilisateur durant le processus de conception. Figure évanescence soumise à des politiques multiples de représentations (Epstein, 2003) afin d'en faire une variable appréhendable par la gestion par projet, le public n'est pas ici compris comme un réceptacle de la production. Il est convoqué, par le biais de ces représentants, en tant que partie à la conception, agi par la projection d'usage. Dès lors, la réduction de l'utilisateur à un utilisateur et à des données constitue la marque d'une réussite particulière. Il s'agit des prémisses d'une forme d'expérimentation au sein de laquelle les

---

<sup>273</sup> Cette notion est à distinguer de la catégorie analytique que nous avons auparavant construite en s'inspirant des travaux de Gabriel Tarde

<sup>274</sup> « The public consists of all those who are affected by the indirect consequences of transactions to such an extent that it is deemed necessary to have those consequences systematically cared for. » (Dewey, 1927 p. 15-16). « Those indirectly and seriously affected for good or for evil form a group distinctive enough to require recognition and a name. The name selected is « The Public. » (Dewey, 1927 p. 35).

concepteurs s'attachent à fixer et stabiliser les variables de leur projection<sup>275</sup>. Ici, ce travail passe par la mise en conformité de la variable au faisceau de solutions et à l'obligation pour ces représentants de ne représenter que l'utilisateur.

---

<sup>275</sup> « There is no mysterious great leap to the public except when one imagines that it is excluded a priori from production and is sufficiently explained by the rules of music, the laws of the marketplace, and the tricks of the trade. According to our analysis, the public is no longer external to music; it remains a variable throughout the equation, when the producers have pushed their trial-and-error method in the studio to its limit and when there is no way of proceeding any further therein. The real public takes the place of the remaining x, when what all this amounts to can be seen. But this does not happen all of a sudden. The public is not an abstraction that comes along (or not) at the end of the route to sanction the work of production: it is a circle of actual auditors that is gradually widened. The groping forward continues, following the trial-and-error procedure that allows one to get closer to a good definition of the public for a given recording. » (Hennion, 1989 p. 416)

## XI - Conclusion de la partie III

---

En explorant les contraintes et opportunités d'observation du scénario et des processus de scénarisation, nous avons amendé notre définition provisoire initiale : d'un *travail de représentation de l'usage de technologie*, nous avons qualifié la projection d'usage de *représentation de l'écologie socio-technique de l'usage*. Les analyses découlant de cette troisième partie nous engagent à modifier à nouveau cette définition et à y insérer la part d'essence fictionnelle qui structure la projection d'usage et la rend performative. La projection d'usage peut dès lors s'envisager comme un ensemble de *représentations de fictions au service de la recherche technologique*. Cette modification permet également de mettre en lumière l'enjeu de la projection d'usage : c'est bien la recherche technologique qui, en en constituant la finalité, conditionne également la matière de la projection. C'est au regard de cette finalité que la rentabilité de l'investissement de forme fictionnelle sera évaluée. Cette mobilisation des ressources par le récit évoque la gestion par la mise en récit – le « *storytelling management* », modalité de gestion caractéristique d'un capitalisme aux formes nouvelles :

« elle consiste à créer des fictions mobilisatrices, à engager tous les « partenaires » (ou « parties prenantes »), salariés et clients, managers et actionnaires, dans des scénarios prémédités. A la place des chaînes de montage, des engrenages narratifs. Plutôt que le contrôle et la discipline, le prétendu partage d'une histoire collective. Le *storytelling management* peut donc être défini comme l'ensemble des techniques organisant cette nouvelle « prolixité » productive, qui remplace le silence des ateliers et des usines : le néo-capitalisme ne vise plus seulement à accumuler des richesses matérielles, mais à saturer, à l'intérieur et à l'extérieur de l'entreprise, les champs de production et d'échange symboliques. Une fois adopté par un service de l'entreprise, le *storytelling* gagne les autres : marketing, communication interne, gestion des « ressources humaines », formation au leadership, stratégie, gestion de projets et, plus surprenant encore, le management financier. » (Salmon, 2007 p. 103-104)

Directement lié à cet impératif de maximisation du profit au regard des ressources allouées, autrement dit du souci du retour sur investissement, la projection d'usage s'établit comme un investissement de forme destiné à sortir le scénario de ses conditions locales de production en le dotant de caractéristiques appropriables par d'autres. C'est à cette condition que le scénario d'usage se fait projection d'usage. Nous allons désormais nous intéresser dans la partie suivante aux actions concrètes et à la mise en œuvre de systèmes de normes



par les concepteurs de la projection d'usage afin de mieux appréhender les mécaniques d'élaboration (de choses, d'objets et de personnes) à l'œuvre lors de la projection d'usage.

## **Partie 4. La scénarisation ou la composition d'axiomes**

*« L'instant d'inspiration semblait être réfléchi maintenant de tous côtés à la fois,  
par une multitude de circonstances nébuleuses,  
de faits qui s'étaient produits ou qui auraient pu se produire.  
Cet instant avait éclaté comme un point de lumière,  
et maintenant,  
sur les nuages superposés des circonstances incertaines,  
une forme confuse apparaissait, voilant suavement la lueur attardée.  
Ah ! Dans le seing virginal de l'imagination, le verbe s'était fait chair. »  
(Joyce, 1992)*

S'intéresser à la projection d'usage commande de se préoccuper plus précisément des conditions de sa production. C'est en portant notre regard sur le processus, que nous avons pu requalifier la projection d'usage comme un *composition d'axiomes*.

Ce constat participe d'abord de l'étude du contexte « *matériel*<sup>276</sup> » de la projection d'usage (XII). Durant le temps de l'observation participante, ce contexte nous est apparu comme sujet à de nombreuses variations et métamorphoses : les choses qui le constituaient se montraient alors d'autant plus foisonnantes qu'elles semblaient changer constamment de statut. Ce constat empirique nous a amenés à nous appuyer sur cet aspect mouvant et évolutif du contexte matériel pour en caractériser, dans l'analyse, les traits saillants. L'objectif ici poursuivi est la caractérisation du processus d'élaboration de la projection, la scénarisation, en tentant d'en retracer une généalogie mineure car microsociologique. La toile de fond conceptuelle de ce chapitre est rivée à la notion d'« *objet-frontière*<sup>277</sup> » (Griesemer & Star, 1989 ; Bowker & Star, 1999) et à certaines réflexions associées.

Dans le chapitre suivant (XIII), nous interrogeons la survenue de tels phénomènes en traquant le « *travail invisible* » à l'œuvre durant le processus de scénarisation. Nous démontrerons que le glissement d'une *expertise stratifiée* à une expertise distribuée a permis aux acteurs de *sauver les apparences* d'une collaboration fondée sur des briques d'expertises par le décroisement de celles-ci. Dans un second temps, nous nous intéressons à la catégorisation comme processus de mises en convergences de choses *a priori* non conciliables par trois phénomènes : la créolisation du langage, la dissémination de l'expression des réflexivités et l'émergence de lieux et de personnes frontières, les *Borderlands*.

---

<sup>276</sup> « Au lieu de nous précipiter dans l'esprit, pourquoi ne pas regarder d'abord les mains, les yeux et le contexte matériel de ceux qui savent. « Matériel » on le voit, ne nous renvoie pas à des infrastructures mystérieuses que seul l'économiste connaîtrait, ou à des agencements de neurones que seul le neurobiologiste connaîtrait, ou à des capacités cognitives que seul le psychologue connaîtrait, ou à des paradigmes que seul l'historien des sciences connaîtrait. L'adjectif « matériel » nous renvoie à des pratiques simples par lesquelles toutes choses sont connues, y compris les économies, les cerveaux, l'esprit et les paradigmes. » (Latour, 1985)

<sup>277</sup> Voir définition page 109

## XII - La scénarisation : co-conception d'une « infrastructure-frontière »

---

Nous commencerons ce chapitre en interrogeant le rôle du scénario, en tant que produit de la projection d'usage (A). En revenant sur le contexte matériel de sa production, nous souhaitons démontrer qu'il participe de la mobilisation d'une écologie d'objets dont les statuts ne sont pas figés et dont les contributions respectives au scénario sont variables. Plutôt qu'un « *objet-frontière* » (Griesemer & Star, 1989), le scénario sera alors compris comme une « *infrastructure-frontière*<sup>278</sup> » (Bowker & Star, 1999).

Dans un second temps, nous poursuivrons l'analyse en adjoignant aux mutations qui animent cette écologie d'objets les trajectoires des personnes qui les manipulent (B). L'étude des interactions entre ces deux phénomènes mettra en évidence l'étroitesse des liens entre les trajectoires empruntées par les objets et celles empruntées par les personnes, les identités des premiers étant dépendantes de celles de ceux qui les manipulent.

A travers cette analyse en deux temps, nous souhaitons démontrer que le travail de projection d'usage est une suite de tests durant lesquels sont mis à l'épreuve les statuts des « *choses*<sup>279</sup> » qui l'agissent. Ces épreuves subies sont autant de moments durant lesquels les dynamiques et la nature des « *attachements*<sup>280</sup> » sont renégociées. En faisant s'entrechoquer des trajectoires d'objets et de personnes, la projection constitue une succession d'épreuves sur le chemin de la constitution d'une infrastructure frontière.

### *A - Le scénario : une infrastructure frontière ultra-locale reposant sur une écologie d'objets aux statuts fluctuants*

Le travail de Charlotte Lee et le concept associé d'artefacts de négociation des frontières, « *Boundary Negotiating Artefact* » (BNA) – des concept qui entre en résonance avec ceux d'« *objet-frontière* » (Griesemer & Star, 1989 ; Bowker & Star, 1999), d'« *objet*

---

<sup>278</sup> En revenant sur le travail de Susan Star sur la notion d'objet-frontière et de travaux adjacents, Dominique Vinck et Pascale Trompette soulignent la mise en visibilité des infrastructures durant les moments d'agitation : « Transparentes et invisibles, elles peuvent être rendues visibles au travers des défaillances, des ruptures ou des épreuves, notamment dans le cours de l'innovation où l'objet-frontière compose avec des architectures existantes. » (Trompette & Vinck, 2009 p. 10)

<sup>279</sup> La notion de « chose » est utilisée par Geneviève Teil afin de se dégager de la distinction entre personnes et objets, humains et non-humains (Teil, 2010)

<sup>280</sup> « Cette notion cherche à analyser l'usage ou la consommation comme le résultat d'un processus réflexif d'interaction avec l'objet sans recourir à des distinctions a priori entre ce que les choses ou les acteurs sont capables ou non d'attacher et comment. La notion d'attachement prend ses distances autant avec le monde des choses, qu'avec celui des acteurs et leurs mises en relation asymétriques respectives. Elle amène à reconsidérer des choses qui s'attachent à nous autant que nous nous attachons à elles et redonne du mystère à la façon dont les uns ou les autres y parviennent. » Synopsis d'un numéro de la revue « Sciences de la société » à paraître sous la direction de Catherine Lejealle et de Geneviève Teil, tiré de la présentation de l'atelier « Arbitrer des attachements », sous l'égide de l'AFS RT 11, « sociologie de la consommation et des usages, les 30 et 31 mars 2010 »

*intermédiaires* » (Vinck, 1995 ; Jeantet, 1998 ; Boujut & Blanco, 2003), de « *prototypes* » (Subrahmanian *et al.*, 2003) - s'inscrit à l'analyse d'un projet au caractère exploratoire et dont la collaboration entre tous les partenaires est inédite :

*« The dependence of boundary objects on the premise of established standards is inherently problematic for theorizing incipient, non-routine, and novel collaborations. Theories are needed to explain how collaborators from different communities of practice, that lack pre-existing standards, use material artifacts to collaborate. The empirical research undertaken for this study follows a newly formed, interdisciplinary design group. Lacking standardized processes and objects for collaboration, the collaborators created what I will call boundary negotiating artifacts. »* (Lee, 2007 p. 315)

Pour l'auteure, les BNA sont utilisés à des fins variées et s'inscrivent dans le prolongement d'artefacts de coordination de travaux collaboratifs :

*« [They] are used to: record, organize, explore and share ideas; introduce concepts and techniques; create alliances; create avenue for the exchange of information; augment brokering activities; and create shared understanding about specific design problems. Boundary negotiating artifacts may be considered to be an extension of previous work on coordinative artifacts such as ordering systems, intermediary objects, and prototypes. »* (Lee, 2007 p. 333)

L'auteure établit que ces objets utilisés et ajustés durant les interactions de groupe ne sont pas un nouveau type d'« *objets-frontières* » malgré la parenté existante avec le concept original. Tandis qu'elle rappelle le fait que les objets-frontières doivent satisfaire aux besoins informationnels de chaque communauté de pratique (Bowker & Star, 1999), Charlotte Lee considère que certains objets échappent à ce spectre définitionnel, les BNA. Elle recense ainsi quatre types d'objets (Lee, 2007) qui ne répondent pas aux exigences du concept d'« *objet-frontière* » :

- les objets qui méritent d'être accompagnés par des discussions et des explications pour être intelligibles
- les objets qui n'ont pas de standards inscrits ou dont les standards inscrits sont incomplets
- les objets qui échouent à satisfaire aux besoins informationnels de toutes les parties
- et enfin, les objets qui jouent un rôle dans les processus de négociation de compréhension mutuelle entre communautés.

Ainsi, l'auteure a considéré nécessaire de forger le concept de « *Boundary Negotiating Artefact* » pour combler le vide analytique concernant ces situations de conception pour lesquelles aucune forme de collaboration durable entre partenaires ni aucune forme standardisée de connaissance ne sont observables.

L'analyse qui va suivre révèle l'incomplétude des éléments constitutifs des scénarios, ce premier constat ouvrant voie à une qualification des scénarios comme « *infrastructure-frontière* » plutôt que comme « *objet-frontière* » (Bowker & Star, 1999) en ce que ceux-ci ne participent ni d'une collaboration durable ni de l'inscription de forme unique de connaissance stabilisée<sup>281</sup>. Ces deux éléments qui structurent l'émergence des « *objets-frontières* » manquent cruellement au projet que nous observons. Ainsi, nous avons considéré la qualification des artefacts qui ont participé à l'émergence des scénarios comme une étape indispensable à l'analyse du travail de coordination menant à la projection d'usage et au scénario.

Nous avons donc pris en compte dans notre analyse des objets, non seulement l'ensemble de ceux qui ont contribué à la production des scénarios, mais également les représentations intermédiaires par lesquelles sont passés les scénarios avant de se constituer en artefact stabilisé. Cette posture analytique est justifiée par notre volonté de ne pas considérer comme donné, c'est-à-dire non susceptible de modification en cours de projet, le statut des objets observés (Verchère & Anjembe, 2010). Il s'agit en effet de ne pas exclure du champ de la négociation (souligné dans la dénomination des BNA) le statut des objets intermédiaires et de ne s'intéresser au final qu'au devenir d'un artefact stabilisé, comme cela fut souvent le cas dans les travaux de la sociologie des techniques.

Notre analyse a permis de regrouper en cinq types d'artefacts les différents objets mobilisés durant le travail de *projection d'usage*. Elle nous a permis d'identifier le fait que ceux-ci puissent avoir des statuts évoluant au fil du travail de scénarisation. En l'espèce, la scénarisation a été rythmée par trois étapes :

- 1) la stabilisation d'une intrigue
- 2) la stabilisation d'une instanciation
- 3) l'émergence de champs du possible.

---

<sup>281</sup> « Another way of talking about boundary objects is to consider them with respect to the processes of naturalization and categorization [...]. Boundary objects arise over time from durable cooperation among communities of practice. They are working arrangements that resolve anomalies of naturalization without imposing a naturalization of categories from one community or from an outside source of standardization. (They are therefore most useful in analyzing cooperative and relatively equal situations; issues of imperialist imposition of standards, force, and deception have a somewhat different structure.) » (Bowker & Star, 1999 p. 297)

Chacune de ces étapes est définie par l'objectivation du scénario en plusieurs formes correspondant à des statuts eux-mêmes différents. Enfin, nous verrons que cette écologie d'objets mouvants est à la base de notre définition des scénarios comme « *infrastructure-frontière* », en tant que production stabilisée de la *projection d'usage*.

### **1) Stabilisation de l'intrigue : la conception d'un « inclusion artefact »**

Commençons-donc par examiner les objets intervenants durant la première phase du travail de scénarisation que nous avons nommée la stabilisation de l'intrigue. Durant cette première phase, deux objets ont un rôle prédominant par rapport aux autres, ce sont l'état de l'art<sup>282</sup> et l'annexe technique<sup>283</sup> au projet. Ils constituent ce que Charlotte Lee nomme des artefacts structurants - « *structuring artefacts* ». Ces objets visent prioritairement à l'organisation de l'activité en fonction de principes considérés comme supérieurs aux autres. Souvent à l'origine de conflits et de disputes, ils ont la particularité d'être peu malléables :

*« Like compilation artifacts, structuring artifacts are used to coordinate media and understanding but, unlike compilation artifacts, structuring artifacts are also used to establish ordering principles, establish tenor in narrative forms, and to direct and coordinate the activity of others. Structuring artifacts were often at the center of heated struggles between communities of practices and were sometimes used to push and negotiate boundaries themselves – quite different from boundary objects which move across boundaries from one community of practice to another with relative ease. »* (Lee, 2007 p. 325)

Dans notre cas d'étude, à plusieurs reprises, les états de l'art provoquent des débats et occasionnent des réajustements marginaux. L'équipe Umanlab signale à plusieurs reprises combien les notions centrales de « *Privacy* », de confiance et de risque méritent d'être stabilisées préalablement à la rédaction des scénarios. Pareillement, le chef de projet insiste régulièrement pour que les scénarios incluent des problématiques liées à la « *Privacy* ». Par ailleurs, le CEA-LETI fournit très rapidement une ébauche très avancée de l'état de l'art des protections technologiques disponibles tandis que les réflexions des autres partenaires demeuraient à l'état de balbutiements. Dès lors, l'accent mis sur les attaques dans cet état de l'art est amené à devenir une variable pesant lourd dans l'élaboration des scénarios jusqu'à en constituer l'intrigue principale. La récurrence de la notion d'attaque et du vocabulaire

---

<sup>282</sup> Voir annexe 2.

<sup>283</sup> Voir annexe 4.



associé (« contre-mesure », « parade », « protection », « danger », « risque ») en est un témoignage frappant.

Dans le même ordre d'idée, l'annexe technique au projet constitue également un document de référence. Au-delà du sobriquet attribué à celui-ci par un des membres de Umanlab (« la bible »), ce document sert de point de référence au chef de projet pour rappeler tant les impératifs de l'organisation prévue que les objectifs principaux du projet.

Ainsi, état de l'art et annexe technique ont été les documents qui ont circulé le plus rapidement dans le projet. Artefacts aboutis ou en état avancé par rapport aux autres productions attendues, ils ont également bénéficié d'une forme de représentation (fichiers électroniques au format PDF) permettant leur diffusion précoce à tous les membres du projet ainsi que leur mobilisation constante. En rappelant chacun des partenaires à leurs engagements, ils ont joué un rôle d'ordonnancement et de priorisation des problèmes à aborder. Ce faisant, ils ont servi de point d'appui à la mise au jour de contradictions ou à l'émergence de volontés contradictoires entre la « *Privacy* » et la sécurité, entre le protocolaire et la couche physique ainsi qu'entre les figures d'utilisateurs à privilégier.

Cependant, malgré la domination de ces objets dans la structuration de l'activité, une autre foule d'objets a servi d'appui à l'action des membres du projet. Représentés la plupart du temps sous la forme de présentations sous format PowerPoint®, il s'agissait de productions internes à chaque équipe : présentation de l'activité de l'équipe, du contexte commercial, synthèse des problématiques de recherche, résumé des principaux résultats, spécificités de la discipline, positionnement socio-économique et notamment présentation des scénarios d'usage par Umanlab<sup>284</sup>. Ces objets constituent ce que Charlotte Lee nomme des artefacts auto-explicatifs - « *self-explanation artefacts* » :

*« The designers used self-explanation artifacts for learning, recording, organizing, remembering, and reflecting. While created and used privately, self-explanation artifacts were sometimes indirectly presented to others through the creation of inclusion artifacts or compilation artifacts. »* (Lee, 2007 p. 319)

Durant cette première étape, le scénario prend déjà une forme intermédiaire. Bien qu'il manque encore de matière et de fond, il est au centre de discussions concernant la forme et le contenu qu'il devait adopter. Construit de manière informelle, le scénario est alors un produit dérivé des scénarios d'usage, stabilisé en tant qu'idée par l'établissement

---

<sup>284</sup> Voir annexe 1, figures 2, 3, 8, 12, 13, 17, 18, 20 à 24.

d'un consensus sur les principaux ressorts dramatiques à mettre en œuvre. Ce faisant, le scénario joue à ce moment le rôle d'artefact inclusif - « *inclusion artefact* » :

*« These were used to propose new concepts and forms. These artifacts were created from self-explanation artifacts and went through an informal screening process of group discussion whereby an idea embodying different concepts and forms (e.g. sketches or text) originating from one community of practice would be proposed to others. This screening process entailed communal gatekeeping whereby the group would use the inclusion artifact as a reference or symbol for the new idea. »* (Lee, 2007 p. 321)

En un sens, la recherche de consensus sur l'idée de scénario est l'illustration d'un processus d'inclusion<sup>285</sup> articulé autour des présentations de chacun des membres du projet (« *self-explanation artefacts* ») et des retours sur chacune d'entre elles :

*« Inclusion artifacts are embedded in a web of practices that can be considered including practices – presenting, accepting, rejecting, and reserving judgment. »* (Lee, 2007 p. 323)

## **2) Stabilisation de l'instanciation : l'émergence d'un « compilation artefact »**

Jusqu'ici, c'était la finalité et l'identité du scénario qui étaient en cours de définition. A partir de cette phase de stabilisation de l'instanciation, le scénario s'est mis à glisser vers un objet auquel tous les partenaires devaient apporter leur contribution. En effet, la frontière entre ce qui relevait du « *technique* » (la sécurité) et ce qui relevait du « *social* » (la « *Privacy* ») a été floutée à mesure que les interactions entre partenaires se multipliaient. L'intrigue est devenue de plus en plus solidaire de son environnement de sorte qu'elle s'est mise à former un système dans lequel l'« *usage* », la « *Privacy* », la « confiance », le « risque » et la « sécurité » étaient des mécanismes enchevêtrés. Leurs définitions étaient contingentes de la personne qui les énonçait et l'énonciation de l'un des termes appelait quasi automatiquement celle d'un autre.

Formellement, le scénario avait pris corps en stabilisant une partie de la technologie : le téléphone portable et les fonctionnalités NFC. Il comprenait d'abord quatre séquences reprenant les quatre « use cases » exposés par Inside et prenait pour cadre le domaine d'application du transport. Ces séquences ont ensuite été requalifiées comme quatre scénarios à part entière en raison des intrigues distinctes qu'elles comportaient.

---

<sup>285</sup> Les tenants de la théorie de l'acteur-réseau auraient certainement parlé ici d'enrôlement.

Ce premier redécoupage a marqué le début de l'intégration croissante d'éléments de nature hétéroclite dans les scénarios. La description des composantes « techniques » du scénario avait gagné en précision tandis que sur le plan de l'environnement, on assistait à une montée en généralités de plus en plus abstraites. L'environnement du premier scénario (« Payment ») s'en est trouvé peuplé d'entités aux contours flous, réduites à des dénominations impersonnelles : Julie aurait tout autant pu s'appeler Juanita ou Jean sans que cela ne bouleverse l'intrigue... Les scénarios sont alors articulés autour d'une séquence narrative à partir desquels des séquences d'action entre utilisateurs et dispositifs techniques étaient déductibles. Chacune de ces séquences a aussi permis de déduire des menaces potentielles.

Ce premier scénario a scellé l'identité des scénarios comme *instanciation de situations d'utilisation* du NFC. Ces situations, cadres contraignants ou habilitants d'« attaques », ne mettaient pas en scène le CPM. En effet, le CPM n'était pas situé au centre de l'intrigue, il en était la résolution, et aucun des partenaires n'était encore prêt à définir plus précisément l'étendue de son rôle. La construction du scénario « Payment » a également fait l'objet d'aller-retour entre différents partenaires.

Ces premières formes d'objectivation du scénario<sup>286</sup> vont peu à peu permettre d'observer la constitution d'un artefact compilant - « *compilation artefact* ». Ceux-ci sont décrits par Charlotte Lee comme des moyens de création de consensus et de communication entre communautés de pratique. Ils se caractérisent également par la courte durée de leur emploi :

« *Compilation artifacts (e.g. tables, technical sketches) were used to coordinate both media and the designers themselves. The designers used compilation artifacts to bring two or more communities of practice into alignment just long enough to develop a shared and mutually agreeable understanding of a problem and to pass crucial information from one community of practice to another.* » (Lee, 2007 p. 323)

Les « *compilation artefact* » se distinguent également par le fait qu'ils agrègent plusieurs types de pratiques de conception :

« *Compilation artifacts are involved in a web of compiling practices: remembering, gathering, organizing, discussing, anticipating needs, presenting, and explaining.* » (Lee, 2007 p. 329)

<sup>286</sup> Voir annexe 1, figures 9 à 11 et 14 à 16.

Ainsi, on retrouve cette capacité d'agrégation, de compilation de pratiques, dans la propension grandissante des membres du projet à s'accaparer tout ou partie des productions qui leur ont été présentées par d'autres membres du projet. On compte parmi ces objets le tableau à double entrée proposé par le CEA-LETI comme moyen de classement des attaques et des contremesures<sup>287</sup>. Umanlab l'a détourné dans l'une de ses présentations comme moyen d'illustration de l'articulation entre « scénarios d'usage » et « scénarios d'attaque<sup>288</sup> ». De même, les dénominations propres à la cryptographie – « Alice », « Bob » et « Charlie », ont un temps été détournées pour dénommer des usagers potentiels du NFC. Les « use cases » présentés par Inside ont également été intégrés par l'équipe Umanlab comme étape du schéma narratif développé. On notera pareillement le fait que l'UVSQ et INSIDE se sont emparées des notions de « trust » et de « confidence » dans leur contribution technique aux scénarios. Aussi, des artefacts ont été empruntés à d'autres entités que celles présentes dans le projet : la définition de la « Privacy » inspirée du HCI dans une des présentations de Umanlab, la suggestion, vaine, d'utiliser un modèle d'évaluation éprouvé en marketing par le chef de projet (le « Technology Acceptance Model »). En empruntant de la sorte à des artefacts cognitifs inhérents à différents champs des sciences pour l'ingénieur, les membres du projet ont procédé à un véritable « travail d'équipement<sup>289</sup> » de l'idée de scénario.

Ces objets exotiques, empruntés et souvent détournés de leur usage orthodoxe, sont dénommés « *borrowed artefacts* » :

*« Borrowed artefacts that are taken from its creator in one community of practice and used in unanticipated ways by those in another community of practice. Designers use borrowed artifacts to augment their understanding of design problems. The practice of borrowing occurs when communities of practice are in close proximity. »* (Lee, 2007 p. 331)

Leur intégration graduelle va aboutir à un redécoupage progressif de l'idée originelle de scénario : d'un schéma narratif rythmé en quatre étapes correspondant aux quatre « use cases » présentés par Inside, le scénario est redécoupé en quatre objets différents, quatre saynètes. Cette requalification des scénarios par les acteurs recoupe leur progression au niveau analytique : d'inclusion artefact, le scénario se meut en compilation artefact,

<sup>287</sup> Voir annexe 1, figure 2.

<sup>288</sup> Voir annexe 1, figure 5.

<sup>289</sup> « Par « travail d'équipement », nous entendons l'activité collective qui consiste à s'accorder sur les éléments qu'il convient d'ajouter aux objets intermédiaires afin qu'ils s'inscrivent dans un espace d'échange entre acteurs plus ou moins hétérogènes. L'équipement des objets intermédiaires vient des acteurs qui gravitent autour de ces objets ou qui les font circuler entre eux. Grâce à cet équipement, certains objets intermédiaires matérialisent et transportent dans l'interaction une infrastructure invisible faite de standards, de catégories, de classifications et de conventions propres à un ou plusieurs mondes sociaux. » (Vinck, 2009 p. 66)

mosaïques de pratiques émergentes et localement situées<sup>290</sup>. Les scénarios servent alors essentiellement de moyen d'ajustement entre l'ensemble des parties en place tandis que leur mission originale est quasiment laissée en friche.

### **3) L'émergence de champs du possible : la consolidation d'une infrastructure-frontière**

Les différents cas possibles sont cette fois-ci accompagnés des réponses possibles du CPM. Les scénarios sont devenus un outil d'évaluation et de description. Le volet descriptif, après avoir fait l'objet d'une traduction des séquences narratives en procédures techniques, est complété par une autre opération de traduction : cette fois-ci, par l'intermédiaire de Umanlab, les procédures techniques sont traduites en séquences d'usage. Cette dernière étape de scénarisation est caractérisée par l'intensité des échanges entre partenaires et notamment entre Umanlab et Inside. C'est dans l'évaluation des menaces et des solutions apportées que la notion de « *Privacy* », déclinée à l'aide d'une utilisation opérationnelle de trois variables (« risque », « contrôle », « feedback »), est la plus mobilisée. En somme, tandis que le concept devait servir de ressource primordiale à l'élaboration des scénarios, il a supporté plusieurs opérations de traduction avant de recouvrer un rôle prépondérant durant l'élaboration de la partie évaluative des scénarios. Ce faisant, la « *Privacy* » a été transformée en concept commensurable traduisant le détachement progressif des scénarios d'une logique de l'usage à une logique d'utilisabilité. Ainsi, la stabilisation de la description de la technologie a déclenché une réapparition des figures de l'utilisateur en contact direct avec le dispositif : opérateurs, industriels, contrôleurs de billets, sociétés de mobilier public.

Cependant, bien que les scénarios aient réussi à fournir une instanciation du fonctionnement du NFC, un inventaire des possibilités d'action du NFC et une grille d'évaluation des enjeux soulevés en termes de « *Privacy* », l'équipe-projet considérait le travail d'évaluation comme étant encore à l'état de balbutiements. Les contributions de Umanlab, lorsqu'elles n'ont pas déçues en ce qu'elles ne constituaient pas un « go/no go », ont été considérées comme un tremplin pour l'élaboration d'une évaluation technoscientifique des propositions. Le document final a eu pour titre définitif « analyse des scénarios » en lieu et place de « spécifications du CPM ».

Ainsi, lorsque se sont engagés des aller-retour entre les scénarios écrits par Umanlab et le travail conjoint d'Inside et de l'UVSQ, les scénarios ont pris un autre statut. En effet,

---

<sup>290</sup> Voir annexe 1, figures 14 à 16.

chacun des pôles de travail va œuvrer « dans son coin » avant d'ajouter sa contribution au document commun. Les scénarios, « *compilation artefacts* », vont prendre une autre épaisseur par l'ajout en son sein de « *self-explanation artefacts* ». Cependant, la particularité de ces nouveaux ajouts à la matière du scénario est que ceux-ci sont tous fondus dans le même moule : tous les objets qui ont concourus depuis le départ à l'émergence du scénario sont devenus à cette étape des « *structuring artefacts* ».

Ainsi, la forme définitive des scénarios s'est trouvée profondément modifiée. Ceux-ci ont été divisés en trois parties :

- les séquences narratives
- les procédures techniques
- l'évaluation du fonctionnement du CPM au regard de la « Privacy ».

Cependant, leur forme est profondément empruntée du poids de quasi standards, les « *structuring artefacts* », élaborés localement à partir d'éléments préexistants et d'éléments nouveaux. Certes, à l'instar des « *objets-frontières* », les scénarios traversent désormais les rigidités des communautés de pratique. Cependant, ils ne s'appuient pas sur une ou plusieurs formes exclusives de savoir et de pratique standardisées : le document créé ne respecte aucun canon disciplinaire<sup>291</sup>. Il navigue entre les eaux de plusieurs régimes de savoirs et s'est saisi de différents instruments relatifs à ceux-ci. Tandis qu'il couvre un large spectre de sources informationnelles, le scénario se caractérise paradoxalement par une réduction de la portée de circulation de l'information produite. La tripartition du document témoigne d'une possibilité d'isoler certaines données afin qu'elles puissent être rapatriées dans leur domaine disciplinaire sans être polluée par le « bruit » d'éléments exotiques mais, malgré cela, ces données demeurent solidaires d'un ensemble structuré par des contraintes nées dans le localisme de la production de la *projection d'usage*.

Cette caractéristique d'*ultralocalité* rend confuse l'identité analytique du scénario (voir chapitre VI) : à la fois centrée vers l'accomplissement de tâches et sur des histoires centrées sur « l'humain », avec des accents d'études d'utilisabilité sans pour autant être inspirés des travaux d'ergonomie, construits sur certaines bases de la conception participative sans représentation directe des utilisateurs, proposant des solutions alternatives à des situations aussi typiques qu'inédites. Pourtant, l'insoumission du scénario à ces classifications existantes<sup>292</sup> n'en annule pas moins la pertinence pour ses concepteurs :

---

<sup>291</sup> Voir annexe 3.

<sup>292</sup> Cf. 0

« Relativement à cette dernière remarque, je me suis légèrement emporté et ai apostrophé mes interlocuteurs en leur demandant la raison d'être du travail d'élaboration des scénarios, des analyses « sociétales », de la volonté de réfléchir au rôle de l'utilisateur et à la notion de « Privacy » : « à quoi sert tout ce qu'on a fait au final, parce que je comprends plus vraiment, quel est le but des scénarios et surtout à quoi ils vous ont servi au fond ? ». Le chef de projet m'a immédiatement répondu : « sans les scénarios, le travail que nous allons entamer n'aurait pas été possible. Sans scénarios, on n'aurait pas d'idées pour le démonstrateur, ni peut être d'idée des utilisateurs. Maintenant, il nous reste à décider qu'elles sont les menaces prioritaires et en fonction de cette décision on va pouvoir savoir dans quelle direction aller pour les spécifications puis pour le démonstrateur du CPM. » Le cryptologue d'UVSQ a ajouté que les scénarios ont permis de « parler sur du concret avec des situations vraies ». Le chef de projet a conclu que « l'objectif ultime est d'intégrer le CPM dans les scénarios et que ça servira peut-être pour les études d'usages de troisième année. » (**Conférence téléphonique (T0 + 20)**)

En effet, le scénario remplit un rôle de « *containers d'idées* », de « *tremplin*<sup>293</sup> » (Bodker & Christiansen, 1997). Le sens de la perspective analytique s'en trouve ici renversé. L'équipe-projet n'est pas partie d'un objet déjà constitué et des pratiques qui l'entourent mais a élaboré un objet, le scénario, à partir des objets versés à sa conception. Les formes de collaboration entre partenaire sont *ad hoc* et les formes de connaissances mobilisées ne sont pas standardisées mais instables et construites dans les échanges locaux. A l'issue de la scénarisation naît ainsi, plus qu'un « objet-frontière », une « *infrastructure-frontière* » construite à partir d'une hétérogénéité d'objets informationnels mis en mouvement par les communautés de pratique parties au projet :

*« Any working infrastructure serves multiple communities of practice simultaneously be these within a single organization or distributed across multiple organizations. [...] Boundary infrastructures by and largely do the work that is required to keep things moving along. Because they deal in regimes and networks of boundary objects (and not of unitary, well-defined objects), boundary infrastructures have sufficient play to allow for local variation together with sufficient consistent structure to allow for the full array of bureaucratic tools (forms, statistics, and so forth) to be applied. Even the most regimented infrastructure is ineluctably also local: if work-arounds are needed, they will be put into place. [...] What we gain with the concept of boundary infrastructure over the more*

<sup>293</sup> « Creating something new is not a matter of deriving from the existing. However, the view that representations are containers of ideas means that there is less of a difference between the new and the present, because it is not a matter of mapping but of containing ideas. » (Bodker, 1998)

*traditional unitary vision of infrastructures is the explicit recognition of the differing constitution of information objects within the diverse communities of practice that share a given infrastructure.* » (Bowker & Star, 1999 p. 313-314)

Cette infrastructure se distingue de la définition de Bowker & Star car elle est construite sur un réseau d'objets à l'identité dynamique. Elle n'est pas le résultat d'une bataille avec une inertie bien en place<sup>294</sup> mais le produit de la scénarisation, processus de négociations entre inerties. Le scénario doit ainsi être compris comme la cristallisation des conditions de commencement de la conception, un *standard ultralocal*<sup>295</sup>, « tremplin » pour la collaboration entre acteurs. Par ailleurs, penser en termes d'infrastructure et de BNA, rappelle à l'analyste la vigilance à observer lors de l'étude de l'innovation. La remise en cause de la stabilité des objets se pose ainsi non comme impératif de succès de l'innovation<sup>296</sup>, mais comme nécessité de traitement des objets de recherche.

Afin de mieux saisir comment ses emprunts et ses agrégations d'idées peuvent émerger, nous allons à présent nous intéresser aux rapports entretenus par les communautés de pratique en présence avec ces objets.

## ***B - La naturalisation de l'infrastructure-frontière***

En utilisant un raisonnement par abduction<sup>297</sup>, nous souhaitons élucider le lien entre les artefacts mobilisés pendant la création du scénario et les pratiques déployées par les acteurs. Le raisonnement est inspiré d'une conclusion de Susan Bodker concernant le statut du scénario comme « *objet-frontière*<sup>298</sup> ». L'auteure considère les représentations du processus de conception comme asymptotiques du concept d'« *objet-frontière* ». Celui-ci est un idéal qui ne peut être atteint mais qui doit être poursuivi. Nous souhaitons tirer parti

<sup>294</sup> « L'infrastructure ne part pas de rien ; elle se bat avec l'inertie de la base installée et hérite de ses forces et contraintes. Les fibres optiques courent le long des voies de chemin de fer ; les nouveaux systèmes sont conçus pour assurer une compatibilité ascendante » (Star, 2007 cité par (Trompette and Vinck 2009)

<sup>295</sup> « When representation has to cross boundaries, a closure is created, and the representation is deliberately taken away from its context and is no longer open and mutable in the same way. » (Bodker, 1998 p. 110-111)

<sup>296</sup> (Löwgren & Stolterman, 2004) expliquent le succès des innovations par le dépassement de méthodes stabilisées dans des champs disciplinaires particuliers pour innover.

<sup>297</sup> « Syllogisme dont la majeure est certaine et dont la mineure simplement probable, entraîne la probabilité de la conclusion. (Aristote en a donné comme exemple le syllogisme suivant : La science peut être enseignée [majeure certaine], la justice est une science [mineure probable], donc la justice peut être enseignée [conclusion dont le présent raisonnement démontre la probabilité. » Grand Larousse Encyclopédique, 1960, p. 13. Comme nous l'avons démontré dans les lignes précédentes, nous optons pour ce type de raisonnement afin de pallier le fait que le scénario ne constitue pas un objet-frontière mais une infrastructure-frontière.

<sup>298</sup> « In a way, I see the definition of boundary objects as the ideal for a design representation: They should be plastic yet robust, weakly yet strongly structured. However, as I pointed out earlier, many traditional descriptions are neither plastic nor robust. Phrased differently, it is difficult to create the necessary closure of the representation before passing it on. » (Bodker, 1998 p. 119)



de ce constat en mettant l'accent sur le processus de scénarisation. Dès lors, on rejoint ici la posture de Kathryn Henderson qui, avec le concept de dispositif d'ébauche - « *conscription device* », a voulu s'équiper d'un outil conceptuel qui se focalise sur le processus et non sur l'objet :

*« To accentuate the role of engineering drawings as network-organizing devices and draw attention to the process of their creation, I have termed a subgroup of inscription devices conscription devices, in that they enlist group participation and are receptacles for knowledge created and adjusted through group interaction aimed toward a common goal. To participate at all in the design process, actors must engage one another through the visual representation of the conscription device. They focus their attention and their communications with one another by referring to it. The conscriptive quality of these visual representations is so strong that participants find it difficult to communicate about the design at all without them. »* (Henderson, 1991 p. 468)

Afin de saisir le processus de création des scénarios, nous avons choisi de nous emparer d'une des ramifications du concept d'« *objet-frontière* » bien que nous ayons auparavant démontré que les scénarios n'en sont pas. Ainsi, nous considérons que si les scénarios tendent vers le statut d'« *objet-frontière* », leur trajectoire officie comme révélateur des dynamiques d'appropriation ou de rejet de cet objet par les communautés de pratique en présence :

*« A better way to describe the trajectory of an object in a community is the one of naturalization. Naturalization means stripping away the contingencies of an object's creation and its situated nature. A naturalized object has lost its anthropological strangeness. It is in that narrow sense desituated —members have forgotten the local nature of the object's meaning or the actions that go into maintaining and recreating its meaning. [...] Objects become natural in a particular community of practice over a long period of time. (See Latour's (1987) arguments in Science in Action for a good discussion of this.) Objects exist, with respect to a community, along a trajectory of naturalization. This trajectory has elements of both ambiguity and duration. It is not predetermined whether an object will ever become naturalized, or how long it will remain so; rather, practice activity is required to make it so and keep it so. The more naturalized an object becomes, the more unquestioning the relationship of the community to it; the more invisible the contingent and historical circumstances of its birth, the more it sinks into the community's routinely forgotten memory. »* (Bowker & Star, 1999 p. 299)

L'analyse du processus de naturalisation du scénario nous permettra également de mieux comprendre la *projection d'usage* effectuée par les acteurs en fonction de leur appartenance à leur communauté de pratique respective et des objets attachés aux pratiques de celles-ci.

Ces communautés de pratique, que nous avons évoquées jusqu'ici sans en préciser les contours, sont des configurations sociales définies par des pratiques et des engagements communs sans nécessairement coïncider avec des divisions organisationnelles. Scientifiques et technologues se déplacent au sein de telles communautés structurées par des conventions d'usages de matériel, de biens, de standards, d'outils de mesure (Lave & Wenger, 1991 ; Wenger, 1998 ; Bowker & Star, 1999). Dès lors, elles sont également caractérisées par l'usage commun d'objets intermédiaires de conception.

L'appartenance à ces communautés (« *membership* ») a des conséquences importantes pour l'analyse. Tout d'abord, les membres d'une communauté de pratique entretiennent une familiarité poussée avec les objets qu'ils utilisent. Cette familiarité, lorsqu'elle est maximale, aboutit à la « *naturalisation* » totale de l'objet :

« *The more at home you are in a community of practice, the more you forget the strange and contingent nature of its categories seen from the outside.* » (Bowker & Star, 1999 p. 295)

Dès lors, la rencontre d'une communauté de pratique avec des objets ou catégories attachés non routiniers provoque l'émergence de tensions. Ces tensions, qui sont médiées par les objets, rejaillissent sur les personnes.

Par ailleurs, la notion de communauté de pratique nous intéresse en ce qu'elle lie à la pratique l'expression d'une pensée sociale<sup>299</sup>. Elle renvoie au rapport dynamique entre pratiques et représentations sociales<sup>300</sup> (Abric, 1994), rapports que l'on retrouve dans la littérature STS à travers l'usage répandu de la notion goffmannienne de cadre : « *cadre de référence*<sup>301</sup> » et « *cadre d'usage*<sup>302</sup> » (Flichy, 2003), « *frames of meaning* » (Collins &

---

<sup>299</sup> « [...] les activités de prédécodage de la situation, le système d'attente et d'anticipations généré par l'existence d'une représentation, le système de catégorisation qui lui est associé, tous ces processus qui permettent à l'individu d'organiser ses expériences subjectives, qui structurent et façonnent l'interaction sociale [...] c'est précisément l'existence – maintenant bien démontrée – de ces processus qui fait que la représentation est une action sur la réalité, et qu'elle peut être en cela à l'origine des pratiques. » (Abric, 1994 p. 221)

<sup>300</sup> « C'est une forme de connaissance, socialement élaborée et partagée, ayant une visée pratique et concourant à la construction d'une réalité commune à un ensemble social. Les catégories servant à la classification des choses sont solidaires des formes de groupement social, les relations entre classes le sont de celles qui organisent la société. » (Jodelet, 1997)

<sup>301</sup> « Le cadre de fonctionnement définit un ensemble de savoirs et de savoir-faire qui sont mobilisés ou mobilisables dans l'activité technique. Ce cadre est non seulement celui des concepteurs d'un artefact technique, mais il est aussi celui des constructeurs, celui des réparateurs et également celui des usagers. » (Flichy, 2003 p. 124)

Pinch, 1982 ; Carlson, 1992) et « *technological frames*<sup>303</sup> » (Bijker, 1993 ; Orlikowski & Gash, 1994).

Nous souhaitons saisir l’ancrage des pratiques communautaires dans des paradigmes de l’activité de conception pour mieux comprendre leur contribution respective au travail de projection d’usage. Pour ce faire, nous nous appuyons sur deux travaux complémentaires : les idéaux-types développés par Hirschheim et Klein (1989) dans leur étude sur le développement des systèmes d’information et l’étude de Clemmensen (2004) sur les pratiques de modélisation des usagers par les professionnels de HCI.

Hirschheim et Klein ont identifié quatre manières différentes d’aborder le travail de conception. Elles sont fondées sur la polarisation de quatre dimensions sur deux axes : objectivisme-subjectivisme et ordre-conflit. La position objectiviste dont le but est d’appliquer des modèles et des méthodes inspirées des sciences naturelles pour l’étude du social s’oppose à la position subjectiviste qui considère l’adoption de méthodes compréhensives comme adaptées aux particularités du monde social. L’autre axe oppose l’ordre au conflit. Le premier met l’accent sur un monde social caractérisé par l’ordre, la stabilité, l’intégration, le consensus et la coordination fonctionnelle. La position du conflit ou de la coercition insiste sur le changement, la désintégration et la coercition. Au croisement de ces deux axes, se trouvent les quatre paradigmes guidant l’action des développeurs informatiques (cf. Figure 39) :

- fonctionnalisme (objectivité-ordre) : l’objectif est de fournir des explications du statut quo, de l’ordre social, de l’intégration sociale, du consensus, de la satisfaction des besoins et du choix rationnel. Comment les éléments individuels d’un système social interagissent pour former un tout intégré en est l’une des problématiques clés. L’archétype du développeur est celui de l’expert ou du roi-philosophe platonicien.
- relativisme social (subjectivité-ordre) : chercher l’explication dans le rayon de la conscience individuelle et de la subjectivité et à l’intérieur du cadre de référence de l’acteur social, opposé à l’observateur de l’action. Le développeur est ici un facilitateur de l’action et de l’échange.

---

<sup>302</sup> « Le cadre d’usage ne se limite pas pour autant à l’activité des usagers. Il s’agit plutôt d’une notion qui renverrait à la valeur d’usage des économistes. Le concepteur, comme l’usager, se pose la question de l’usage. » (Flichy, 2003 p. 126)

<sup>303</sup> « The technological frame of a social group is shaped while an artifact, functioning as exemplar, further develops and stabilizes within that social group—the social impact side of the coin. But a technological frame in turn also determines (albeit to different degrees, depending on the degree of inclusion different actors have in that frame) the design process within that social group—the social shaping side of the coin. Thus forms the concept « technological frame » a hinge between the social impact and the social shaping perspectives on technology. » (Bijker, 1992 p. 98)

- structuralisme radical (objectivité-conflit) : ici, l'accent est mis sur le besoin de transcender les limites placées dans les arrangements sociaux et organisationnels. Le développeur s'affirme comme militant du progrès social.
- Néohumanisme (subjectivité-conflit) : l'objectif est la recherche du changement radical, de l'émancipation. Le développeur se pose ainsi comme une figure émancipatrice.

*Figure 39. Paradigmes guidant le travail de conception (Hirschheim & Klein, 1989)*

Paradigme	Archétype du développeur	Développement du système d'information	Éléments utilisés pour définir le système d'information
Fonctionnaliste	Expert ou roi-philosophe platonicien	Exogène, par l'application de concepts formels à l'aide d'outils et de méthodes rationnelles. Intervention planifiée.	Gens, logiciels, ordinateurs, procédures organisationnelles comme entités objectives physiques ou formelles
Relativisme social	Catalysateur ou facilitateur	Endogène, par l'amélioration de la compréhension subjective et de la sensibilité culturelle en s'adaptant aux forces internes du changement social	Subjectivité des significations, des structures symboliques affectant l'évolution du faire, du penser et du partage des deux
Structuralisme radical	Partisan ou défenseur du progrès social	Exogène, en mobilisant une conscience idéologique par l'organisation d'actions politiques et l'adaptation des outils et des méthodes aux intérêts des diverses classes sociales	Gens, logiciels, ordinateurs, procédures organisationnelles comme entités objectives mises au service des intérêts économiques de classe
Néohumanisme	Emancipateur ou thérapeute social	Endogène, en améliorant la compréhension humaine et la rationalité de l'action à travers l'émancipation et la libération des opprimés	Gens, logiciels, ordinateurs, procédures organisationnelles comme entités objectives  Subjectivité des significations et intersubjectivité du langage utilisé

Nous avons observé que ces quatre paradigmes, que l'on peut associer à des « *technological frames* », sont utiles à décrire la manière dont les acteurs du projet envisageaient leurs rôles respectifs. Cependant, à l'instar de ce que nous avons constaté lors de la caractérisation des objets, il nous a semblé utile de considérer le dynamisme de ces rôles durant la scénarisation. Nous avons, pour ce faire, compléter notre grille de lecture par une autre source nous permettant d'appréhender au plus près la représentation qu'ont les acteurs de l'usage de la technologie en développement, le CPM. Ainsi, dans son étude portant sur la modélisation des utilisateurs par les professionnels du champ du HCI, Clemmensen (2004) a identifié quatre idéaux-types de modélisation de l'utilisateur<sup>304</sup> chez ces professionnels :

- L'« analyste » décrit la personnalité du l'utilisateur comme étant abstraite et pluridimensionnelle. Son travail n'est pas restreint à la description des besoins de l'utilisateur mais s'étend à la description de leur personnalité.
- Le « concepteur » modélise les utilisateurs comme des entités concrètes et considère le contexte d'utilisation comme important : « *The 'designer' builds users as models, characters or small figures, which are similar to real flesh-and-blood people with lots of details and a rich environment.* »
- Le « développeur » conceptualise l'utilisateur comme une donnée. Ce faisant il s'intéresse moins à ce que l'utilisateur est censé faire qu'à l'analyse des propositions de conception à partir de méthodes structurées. L'utilisateur est ici considéré comme une partie du dispositif technique.
- Le faiseur de pont - « Bridge builder » décrit l'utilisateur en termes de tâches à effectuer. Il est hanté par l'idée d'obtenir des informations sans rapport avec ses objectifs.

En considérant d'une part, le « *technological frame* » dominant chez les communautés de pratiques en présence puis en identifiant la progression éventuelle dans les rôles observés, nous souhaitons aborder la double question de la naturalisation et de l'affiliation chez ces communautés en prises avec la projection d'usage (voir Tableau 7). Voici les résultats de l'analyse.

<sup>304</sup> L'auteur reconnaît l'existence d'un lien avec d'autres structures conceptuelles telles que les « *schemata mentaux* » (Chevalier and Ivory, 2003), les « *paradigmes* » (Hirschheim and Klein, 1989) et bien entendu, les « *frames of reference* » (Orlikowski and Gash, 1994)

- **Le CEA-LETI : un « technological frame » fonctionnaliste et un rôle de « développeur »**

La distinction opérée entre « peurs fondées » et « peurs fantasmées » est une illustration éloquent du paradigme fonctionnaliste qui guide l'action des membres du CEA-LETI. Pour eux, l'utilisateur fait partie du système. C'est une entité passive (les données personnelles) ou active (les actions qu'il peut déclencher sur le système) qui au mieux, améliore le système, au pire, ne doit pas en déranger le bon fonctionnement. Cette capacité de nuisance de l'utilisateur est allégoriquement représentée par le personnage de Gaston Lagaffe, utilisé lors d'une présentation<sup>305</sup>. Ainsi, l'innovation est envisagée comme une mise en ordre d'entités objectives, la subjectivité des acteurs étant mise à la marge du fonctionnement du système.

En cohérence continue avec ce « *technological frame* », le CEA-LETI a constamment endossé le rôle de « développeur ». Il a incité les autres acteurs à l'adoption de méthodes structurées ou de propositions de conception à analyser. Le CEA-LETI s'est assuré que l'évaluabilité des scénarios en fonction de critères « objectifs » soit l'horizon des modalités de leur constitution.

**Naturalisation**

Tandis que l'indétermination de la technologie NFC a constitué une forme de contingence non embarrassante pour le CEA-LETI, le processus de naturalisation de l'objet scénario s'est heurté à l'inadéquation entre l'acception de la « Privacy » du CEA-LETI et celui de Umanlab. Au départ, largement en retrait de l'élaboration des scénarios, le CEA-LETI a marqué ses interventions par la volonté d'obtenir des grilles de lecture de la « Privacy » en adéquation avec son « *technological frame* » : la « Privacy » comme une entité objective, abstraite et universellement identifiable dans le système. Cette « donnée » devait également pouvoir être identifiable relativement rapidement par des experts du « social ». En somme, c'est la stabilisation de l'instanciation du scénario qui a réellement enclenché le processus de naturalisation de celui-ci. En revanche, les questions relatives à l'environnement de l'intrigue ne les intéressent pas, puisque l'intrigue suffit à répondre à leurs besoins informationnels.

Cependant, il faut noter que ces manières de faire n'induisent aucunement un désintérêt pour la chose « sociale ». En voulant mettre l'accent sur les attaques « dans la rue » plutôt que sur celles en « labo », en s'intéressant à ce en quoi consiste la sociologie ou

---

<sup>305</sup> Voir annexe 1, figure 1.

encore en souhaitant prioriser les attaques intéressant Inside, le CEA-LETI a démontré une certaine forme de curiosité, sinon d'intérêt, pour l'environnement de l'intrigue. Il n'en est pas moins resté confiné dans son rôle de « développeur ».

- **L'UVSQ : un fonctionnalisme exacerbé par un rôle de développeur puis tempéré par un rôle d'analyste**

Dans les présentations données par l'UVSQ, l'usager est une entité abstraite qui échange des données : « Alice », « Bob » et « Charlie ». Ceux-ci doivent leur existence à celle d'une attaque potentielle, venant menacer un ordre à sauvegarder. Cependant, une nuance subtile existe entre cette approche et celle du CEA-LETI : tandis qu'au CEA-LETI, l'utilisateur fait partie du dispositif technologique, pour l'UVSQ, il représente un dispositif technologique qui échange des données avec un autre. Ainsi, l'utilisateur doit être nommé, qualifié *a minima* comme un attaquant (« Charlie ») ou un utilisateur de plein droit (« Alice » ou « Bob »). Par ailleurs, bien que centrée exclusivement sur la notion de sécurité, l'UVSQ établit une distinction presque platonicienne entre l'esprit et la matière : la différenciation entre couches physiques et protocolaires n'est pour l'UVSQ qu'idéelle.

### **Naturalisation**

Tandis que la transformation du scénario comme forme d'instanciation d'une menace marque un premier pas vers la naturalisation, pour l'UVSQ, la « *Privacy* » ne constitue pas un frein en soit à la naturalisation des scénarios notamment, parce qu'elle en est le pendant (idée que la « *Privacy* » s'oppose à la « sécurité »).

Cependant, le processus de naturalisation a été accéléré de deux manières. D'une part, l'UVSQ, en partenariat avec Inside, a pleinement participé à la rédaction des scénarios et ce, dès l'étude de la faisabilité technique des ébauches présentées par Umanlab. Par ailleurs, ce travail de collaboration a porté sur l'exploration de procédures techniques sur le plan protocolaire alors que sur le plan des couches physiques, le CEA-LETI avait avoué avoir une idée déjà avancée de ce que pourrait être le CPM. Ainsi, les scénarios, objets étranges au départ, sont devenus objets de création et d'implication au fil du temps.

- **Umanlab : le paradigme du relativisme social, le passage d'un rôle de « designer » à celui de « bridge builder »**

Le travail de Umanlab a été tout entier axé sur la présentation de la « *Privacy* » comme une notion contingente et sur la nécessaire prise en compte des subjectivités dans

l'appréhension de cette notion par les usagers. Cependant, ce rôle de « *designer* » s'est progressivement effacé au profit de celui de « *bridge builder* ».

### **Naturalisation**

L'objet scénario peine à être naturalisé dès le départ. En réalité, lorsque l'équipe se conforme originellement à l'idée qu'elle se fait des scénarios, conformément à une pratique *pythique* de l'usage, cela constitue un blocage. Pour les sociologues, l'indétermination de la technique ajoute à l'inexistence du *public*.

Le processus de naturalisation de l'objet en devenir va réellement s'amorcer à partir du moment où l'équipe va se mettre à emprunter des outils et concepts : les menaces présentées par le CEA-LETI ou encore la définition de la « *Privacy* » empruntée au HCI. Dans le même temps, l'équipe presse pour qu'au moins un élément, la « technologie » (le téléphone portable), puisse être stabilisée *a minima* (à la différence de l'utilisateur). Cette nécessité de matérialiser la technique se retrouve dans la proposition de Umanlab de distinguer des scénarios en deux groupes : ceux intégrant une technologie autonome et ceux mettant en scène une technologie à intégrer dans un dispositif existant, le téléphone. Dans le même ordre d'idée, c'est toujours le téléphone qui leur permet de naturaliser le NFC. Cette nécessité de rallier la technologie à de l'existant explique les diverses suggestions et raisonnements par analogie de Umanlab comme l'évocation des virus informatiques ou encore des SPAMs.

Cette politique d'emprunts participe de la volonté de surmonter cet obstacle pour se familiariser avec un scénario... nécessairement conforme aux attentes informationnelles des autres partenaires. La stabilisation du « social » ne se jouera alors qu'à posteriori, bien après la constitution de l'état de l'art dont l'équipe avait la charge.

Dans le cas de Umanlab, il faut noter que la naturalisation des scénarios par le responsable projet n'a pas atteint le même degré d'intensité que pour les deux autres personnes impliquées. En témoigne, sa réaction d'incompréhension de la discussion ayant eu lieu lors de l'ultime réunion téléphonique.

### **- Le structuralisme radical d'Inside : d'« analyste » à « Bridge builder »**

L'entreprise Inside, de part ses ambitions commerciales, ancre l'utilisateur dans et hors le dispositif technique. Son premier apport au projet en atteste : il s'agissait d'une présentation



des applications, « use cases », du NFC. La volonté d'Inside de « coller » au marché vient en contrepoint de l'autre versant de l'expertise apportée par ses représentants, la cryptologie.

### **Naturalisation**

C'est Inside qui entérine le téléphone portable comme dispositif d'utilisation du NFC. Tout d'abord faiblement impliqué dans la construction du scénario en raison de la succession d'interlocuteurs différents en début de projet, le rôle d'Inside s'est métamorphosé en profondeur dès lors que leur équipe s'est stabilisée.

Malgré une naturalisation rendue aisée par la présence dans les scénarios de leurs domaines d'application et des modes d'utilisation du NFC, l'un des représentants d'Inside (doctorante) a illustré, par ses interventions, le rôle d'« analyste » joué par l'industriel au départ comme l'atteste sa critique de l'absence de « *Privacy* ». Cependant, l'entreprise, du fait de l'implication d'un autre doctorant va ensuite endosser le rôle de « *Bridge builder* » pour des raisons identiques que celles de l'UVSQ.

Tableau 7. Trajectoires des communautés de pratique

	Paradigme	Rôles	Statuts des objets mobilisés	Moment catalyseur de naturalisation
<b>CEA-LETI</b>	Fonctionnaliste	Développeur	Structuring artefacts	Emergence de champs du possible
<b>UVSQ</b>	Fonctionnaliste fort	Développeur	Structuring artefacts Self-explanation artefacts	Stabilisation de l'instanciation
	Fonctionnaliste doux	Analyste	Structuring artefacts Borrowed artefacts	Emergence de champs du possible
<b>Umanlab</b>	Relativisme social	Designer	Self-explanation artefacts	Stabilisation de l'intrigue
		Bridge builder	Structuring artefacts Borrowed artefacts Self-explanation artefacts	Stabilisation de l'instanciation
<b>Inside</b>	Structuralisme radical	Analyste	Structuring artefacts Self-explanation artefacts	Stabilisation de l'instanciation
		Bridge Builder	Structuring artefacts Borrowed artefacts	Emergence de champs du possible

Au-delà d'une explication par les « *frames of meaning* » de cette séquentialisation différenciée des processus de naturalisation selon les communautés de pratique, nous souhaitons compléter l'analyse en prêtant attention au statut des productions du travail pour chacun des acteurs. Autrement dit, en examinant les *intérêts à agir* de chacun d'entre eux, il

est possible de comprendre les freins et moteurs du processus de naturalisation en fonction de la capacité des artefacts à répondre favorablement à la satisfaction en besoins informationnels des communautés de pratique. Pour ce faire, nous nous sommes intéressés aux modalités de dissémination des résultats (voir figure 40)

Figure 40. WP5, tâche 2. (Extrait de l'annexe technique au projet)

WP5 Task 2		Title : Dissemination of results			
Start	T0+12	Duration	24 Months	Resources (m.m)	12
Partners		INSIDE	CEA-LETI	UVSQ	UPMF
Effort in m.m		1	3	6	2
Objectives : To disseminate the projects results through papers, seminar and web site					
Description of work:					
Description of work					
<ul style="list-style-type: none"><li>- Write papers describing the results and work of the project to international conferences or workshops to be identified (CHES, ...)</li><li>- Participation to congress (Cartes 200X)</li><li>- Validation of publications according to the confidentiality policy of the project</li><li>- Contribution to contactless PET standardization</li><li>- Workshops with consumers associations and public organizations involved in privacy</li></ul>					
Deliverable	Title			Date	Type
D 5.2.1	Papers, workshop, ....			T0+36	X
Validation criteria: Accepted papers, seminar organization					

Le travail de dissémination des résultats, certes, tient d'une certaine forme d'expression et de publicité conventionnelle des éléments de réussite du projet, mais il répond à des intérêts et à des manières de faire différentes, sinon contradictoires. Le CEA-LETI a toujours été traversé par des tensions de finalité concernant la priorisation du dépôt de brevet ou celle de production de publications académiques, l'une n'étant bien entendu pas sans lien avec l'autre. La PME Inside est bien plus impliquée dans la participation aux salons professionnels et autres types de rendez-vous dédiés aux enjeux liés à la standardisation et la commercialisation des dispositifs sans contacts qu'à la valorisation académique de leur travail. L'entreprise fait d'ailleurs partie intégrante du NFC forum. Les universitaires de l'équipe Prism de l'UVSQ sont eux, cela tient quasiment de la tautologie, principalement intéressés par la valorisation académique. Enfin, l'équipe Umanlab est alors constituée de personnes, qui dans le cadre du projet, privilégient un déploiement d'énergie orienté vers la reconnaissance de leur statut d'expert plutôt que vers les formes consacrées de publicité

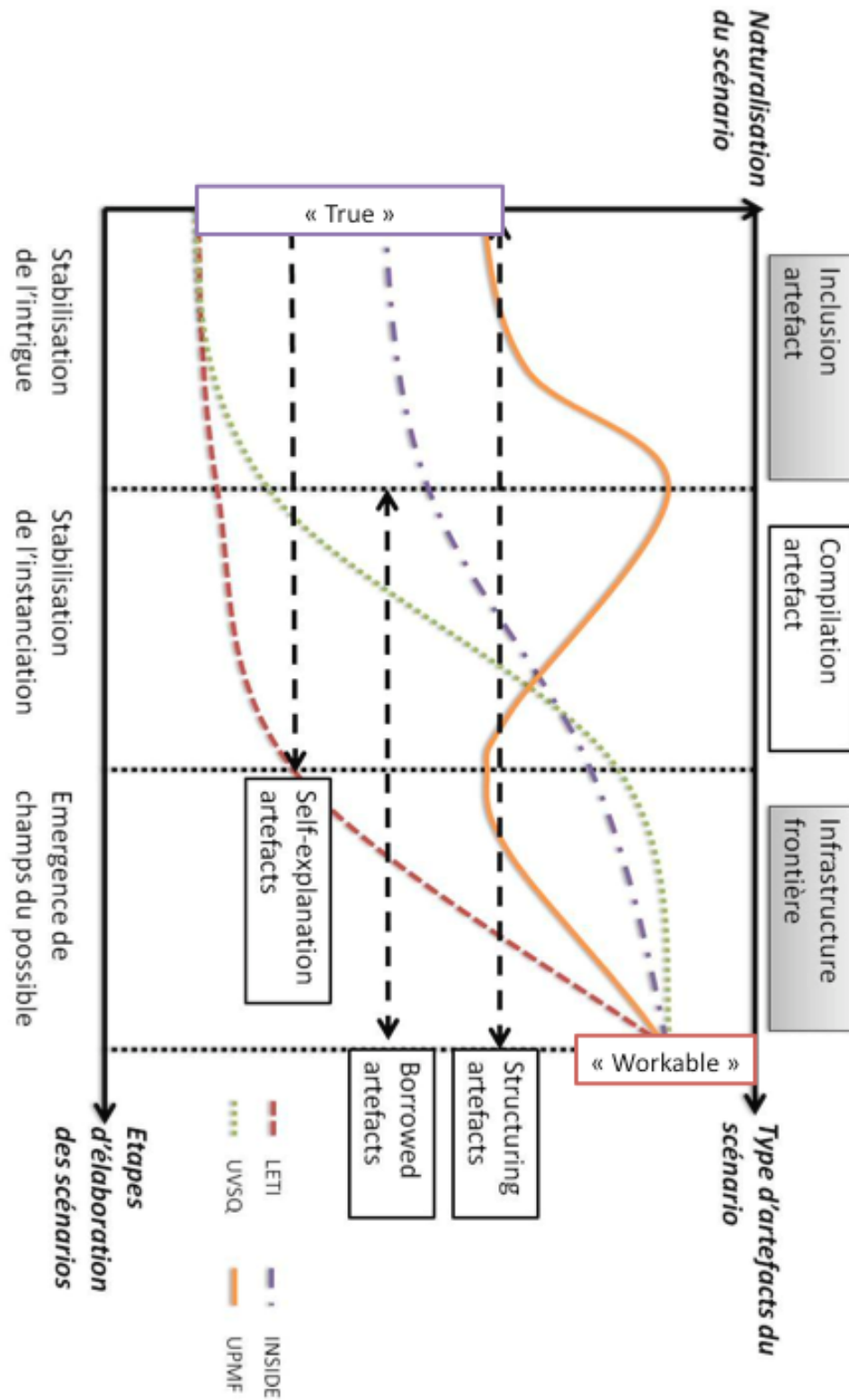
dans les champs académiques. Notons par ailleurs que les règles présidant à la valorisation académique des travaux relèvent de contraintes disparates selon les champs disciplinaires pris en compte (temporalité des appels à communication et à publication différentes, diversité des critères de sélection, porosité entre monde académique et monde socio-économique, etc...). Cette brève description des différences entre intérêts à agir dans le projet et arènes dans lesquelles s'exprimer à l'extérieur du projet pour chacun des partenaires permet d'appréhender les différences de naturalisation en fonction de l'« accountability » perçue des productions (Shapiro, 1994 ; Blomberg, Suchman & Trigg, 1996). Cette accountability fait entrer en concurrence les notions d'actionnabilité et de vérité, de « workable » et de « true<sup>306</sup> » selon les identités professionnelles des acteurs (Wagner, 1997). En effet, les premières productions du projet (« self explanation artefacts » et « structuring artefacts » par certains aspects) tiennent de la démonstration d'une recherche accomplie de vérité (true), vérité non contestée par les autres parties en tant que telles (en tant que « science ») mais non appropriables car ne répondant pas aux besoins informationnels de l'ensemble des partenaires. Or, à mesure que le processus de naturalisation s'intensifie, les productions deviennent de plus en plus exploitables dans le projet (workable) par une prise de liberté maîtrisée avec les canons d'expression relatif aux sciences en jeu. En somme, dans le cadre du projet, dire le vrai fonde la crédibilité des acteurs mais c'est l'énonciation de l'actionnable qui suscite l'effectivité de la collaboration (voir figure 41). Cette effectivité s'établit par une forme de renonciation aux frontières des « technological frames » respectifs et par la constitution d'un « technological frame » commun, propre au projet et générateur d'une « infrastructure-frontière » ultralocale.

---

<sup>306</sup> « The « workable versus true » distinction is tightly connected to questions of accountability. Accountability not only depends on the roles and responsibilities a person assumes, but also on what is considered the most relevant outcome of a project: Academic publications that will be reviewed by a highly specialized community of researchers; a prototype that acts as an approximation of a future product or rather helps users and developers to explore opportunities. In multidisciplinary design projects, participants may find themselves immersed in conflicting roles, structures of accountability, and conceptions of what is relevant. Their discussion is made difficult by the ambiguous character of definitions of what « true » or « workable » means. Some of this ambiguity results from the uncertainties involved in translating an ethnographic description into design decisions. Additional inconclusiveness arises from the fact that particular design decisions are only loosely coupled to how a fully developed and implemented system will affect work at a particular site. On one hand, it is clear that through the technical features of the system -- the language in which it has been developed and the social conventions that have been frozen in it -- potential uses are prescribed (and others excluded). On the other hand, a system is only partly formed and its uses and implications will vary according to the particular ways it is implemented and how the work practices surrounding it will develop. » (Wagner, 1997 p. 424)

Figure 41. Trajectoires des objets, trajectoires des communautés

Indications de lecture : En ligne, les trois temps du travail de scénarisation. En colonne, les principaux objets mobilisés durant ce travail. A l'intersection des colonnes et des lignes, les cases désignent le type d'artefacts mobilisés selon la typologie de Charlotte Lee. Les changements de ton d'une ligne à l'autre signalent des variations de type d'artefact pour un même objet.



### XIII - La scénarisation : articuler et catégoriser les déplacements

---

Dans les chapitres précédents, nous avons mis en lumière le fait que le travail de projection d'usage soit contraint à répondre à l'exigence d'un *enthousiasme technologique*. Nous avons également pu observer la manière dont cette contrainte servait de soubassement au travail de classification du monde à l'œuvre. Enfin, nous avons démontré que ce travail de projection mobilise des hommes et des objets dont les multiples interactions (inter et intra) bousculent positions et statuts originaux : l'appropriation (la naturalisation) de la *projection d'usage* suscite déplacement et modification chez ce(ux) qui y est/sont engagé(s). Ainsi, le scénario, « *infrastructure frontière* », est également une forme terminale et cristallisée des « *arrangements des acteurs* » (Chalas, Gilbert & Vinck, 2009) avec l'incertitude engendrée par la flexibilité interprétative<sup>307</sup>. Nous désirons, dans ce chapitre, interroger la survenue de tels phénomènes en traquant les interstices inaudibles de leurs réalisations. Quel « *travail invisible*<sup>308</sup> » se met en place durant la scénarisation ? Pour répondre à cette question, nous prendrons comme témoin du « *production work* » (Strauss, 1988) l'organisation officielle du travail de coopération avant de rendre compte de la manière dont les choses ont pu continuer de fonctionner malgré ces écarts au programme original (A). Nous démontrerons alors que le glissement d'une *expertise stratifiée* à une expertise distribuée a permis aux acteurs de *sauver les apparences* d'une collaboration fondée sur des briques d'expertises par le décroisonnement de celles-ci. La particularité de ce « *travail d'articulation*<sup>309</sup> » (Gerson & Star, 1986 ; Strauss, 1988 ; Schmidt, Kjeld & Bannon, 1992), travail de gestion des conséquences de la coopération, est qu'il soulève le voile d'invisibilité sous lequel il est ordinairement dissimulé, en l'espèce, l'organisation par *expertise stratifiée* du projet. Dans un second temps, nous nous intéresserons à la

---

<sup>307</sup> « Demonstrating the interpretive flexibility of an artifact amounts to showing that one seemingly unambiguous " thing " (a technical process, or some material contraption of metal, wood, and rubber as in the case of the bicycle) is better understood as several different artifacts. Each of the different artifacts hidden within that seemingly one " thing " can be traced by identifying the meanings attributed by the relevant social groups. The concept of interpretative flexibility is crucial in countering technical determinism. Indeed, to recognize the interpretative flexibility of artifacts is synonymous with refuting technical determinism. Hence the concept's key role in the social studies of technology: Technical development can be subjected to social analysis only when it can be seen as being not autonomous and not driven by purely internal dynamics. The use of the concept of interpretative flexibility is thus the *raison d'être* of the social studies of technology, the justification for its existence. » (Pinch, 1993 p. 118)

<sup>308</sup> « What is the name for this work of managing the overheads and anomalies caused by multiple memberships on the one hand and multiply naturalized objects on the other? Certainly, it is invisible. Most certainly, it is methodological, in the sense of reflecting on differences between methods and techniques. » (Bowker & Star, 1999 p. 310)

<sup>309</sup> « Articulation work is richly found for instance in the work of head nurses, secretaries, homeless people, parents, and air traffic controllers, although of course all of us do articulation work to keep our work going. [...] Other aspects of cooperative work concern novelty and the ways in which one person's routine may be another's emergency or anomaly (Hughes 1970), or in the words of Schmidt and Simone (1996) both the consequences and the division of labor of cooperative work. The act of cooperation is the interleaving of distributed tasks; articulation work manages the *consequences* of this distributed aspect of the work. » (Bowker & Star, 1999 p. 310)

catégorisation comme processus de mises en convergences de choses *a priori* non conciliables (B).

### ***A - Le travail d'articulation : la distribution de l'expertise entre les strates***

Le passage en revue des participants au projet permet de comprendre ce dernier comme ayant été pensé à partir d'un principe d'*expertise stratifiée*, soit *l'organisation d'un faisceau de solutions adaptées à une situation construite comme problématique et requérant plusieurs savoirs de spécialistes qui se traduira par une somme d'avis relatifs à chacun de ces savoirs, donné à un ou plusieurs mandants, afin qu'il(s) puisse(nt) prendre une décision*<sup>310</sup>. Ainsi, la valeur ajoutée du consortium réside dans la cohabitation productive de partenaires aux champs d'expertise distincts et complémentaires comme l'atteste l'annexe technique au projet :

« The consortium is well balanced with the presence of an SME involved in contactless products for secure applications, a public laboratory involved in applied research on contactless and secure electronic systems and an academic laboratory specialized in cryptography. » (2008 p. 37)

La description du rôle de chacun des partenaires au projet consolide cette approche en *strates d'expertise* :

- La PME Inside est décrite ainsi : « Inside will bring to the project COPRIM its expertise and know-how in design and manufacturing of secure contactless products. INSIDE will address both hardware and protocol aspects. »
- Le CEA-LETI : « will bring in the project its expertise in near field communication, contactless interface design, secure specifications and electronic integration. CEA-LETI will mainly address the physical level and hardware implementation of the [...] project. »

---

<sup>310</sup> Cette définition est construite à partir de celle de l'expertise établie par Yves Trépos, définition dotée d'une certaine autorité académique : « l'expertise ce serait : une situation problématique (une difficulté, qui ne peut être surmontée par l'exercice professionnel normal, voire une difficulté que l'on n'arrive pas à localiser), requérant un savoir de spécialiste (...), qui se traduira par un avis (...), donné à un mandat (qui donne pouvoir à l'expert, éventuellement, de sortir du cadre habituellement autorisé), afin qu'il puisse prendre une décision (...) » (Trépos, 1996 p. 5)

- L'UVSQ : « UVSQ will offer its well established competences in cryptography and secure protocol. UVSQ will address mainly the protocol development of the project »
- L'UPMF (Umanlab) : « UPMF will bring its large expertise in social sciences and basically in innovation and new technologies acceptance by end users (CAUTIC method – User Aided Design for Innovation. »

Le projet est ainsi découpé en niveaux d'intervention relatifs à un expert dédié. La PME Inside jouit du privilège d'intervenir à la fois sur les couches physiques et protocolaires, le CEA-LETI se concentrant sur la première, l'UVSQ doit sa présence à sa compétence dans le domaine cryptographique (couche protocolaire) tandis que l'UPMF est désignée comme organisation experte en sciences sociales appliquées à l'innovation. Ainsi, chaque participant occupe des positions<sup>311</sup> censées contribuer de manière concourante à la réalisation des objectifs du projet.

L'extrait d'entretien qui suit pointe à la fois la place prépondérante de la figure de l'expert dans les projets bénéficiant d'un financement de l'ANR et l'importance de l'énonciation de la problématique générant les besoins en expertise.

« **Umanlab** : D'accord. Lorsque vous aviez répondu à l'appel d'offre, donc, enfin, c'était un appel d'offre ANR...

**Responsable projet CEA-LETI** : C'est ce que l'on appelle un projet ANR, tout à fait, oui.

**Umanlab** : Vous aviez, donc vous n'aviez pas intégré une partie des sciences humaines et sociales dans le projet ? C'est l'ANR qui a...

**Responsable projet CEA-LETI** : Parce que, à l'époque, tout à fait, c'est l'ANR qui nous l'a suggéré. Parce qu'à l'époque, il ne m'est pas venu à l'idée que dans un projet, on va dire, technologique, on puisse introduire d'emblée, un partenaire SHS. C'est, la connexion n'était pas faite à l'époque.

**Umanlab** : Et donc quand l'ANR vous a demandé ça, est-ce qu'ils avaient formulé des choses claires comme l'intérêt d'intégrer des sciences humaines et sociales, les objectifs ciblés, les...

<sup>311</sup> « On ne tiendra donc pas l'expertise pour une profession mais pour une position. » (Trépos, 1996 p. 17). L'auteur consolide par la suite l'opposition de l'expertise à la notion de profession en la dialectisant, l'expertise devenant une « position d'extra-territorialité professionnelle. » (Trépos, 2001 p. 100)



**Responsable projet CEA-LETI :** Vu la position du projet, l'ANR nous a recommandé d'intégrer, plus que suggéré...

**Umanlab :** Ah oui.

**Responsable projet CEA-LETI :** ...nous a recommandé d'intégrer un partenaire des sciences humaines et sociales.

**Umanlab :** D'accord.

**Responsable projet CEA-LETI :** Et je pense que l'idée a dû faire son chemin, puisque dans certains appels d'offres ANR, il ne peut y avoir que des projets même si c'est dans un domaine technologique, il peut y avoir des projets très orientés sciences humaines et sociales.

**Umanlab :** D'accord, ok, oui, d'accord.

**Responsable projet CEA-LETI :** Pas systématiquement, mais de plus en plus, on voit apparaître, dans les appels d'offres ANR, en particulier pour la sécurité globale, les systèmes de sécurité globale, la recommandation d'intégrer des personnes de sciences humaines et sociales.

**Umanlab :** D'accord. Donc l'ANR vous fait cette recommandation. Après, ça se passe comment ? Vous faites un appel d'offres ? Ou c'est par...

**Responsable projet CEA-LETI :** Alors, en fait, chaque année, l'ANR, sur un certain nombre de thématiques, il y en a de plus en plus, une trentaine maintenant, peut-être, peut-être même plus. Sur un certain nombre de thématiques, l'ANR émet des appels à projets. En général, c'était mis au courant janvier. Et puis, il faut rendre sa copie fin mars ou courant avril.

**Umanlab :** D'accord.

**Responsable projet CEA-LETI :** Et puis le projet démarre en général en janvier de l'année suivante, s'il a été labellisé. Puisqu'il y a une période d'évaluation des projets et de sélection des projets qui vont être financés, à la fin du printemps, début de l'été, fin juillet.

**Umanlab :** Oui, d'accord.

**Responsable projet CEA-LETI :** Et donc, suite à ce processus d'évaluation, en septembre, on a reçu les recommandations en septembre 2007. On a reçu les recommandations des experts, qui nous ont demandé de rajouter en partenaire, SHS. Mais le

projet avait déjà été labellisé, c'est-à-dire, qu'il avait déjà, il était accepté. Il était déjà accepté.

**Umanlab :** D'accord, oui, d'accord. Donc, après, du coup, c'était plus souple pour choisir, par exemple, les gens de...

**Responsable projet CEA-LETI :** Oui, c'était à nous à proposer, et puis eux, ils ne nous ont jamais dit non. Donc, ils nous ont dit oui. Mais ils ont accepté ce nouveau partenaire, donc, qui avait toutes les qualités pour faire le projet, puisque, un de ses laboratoires, que vous connaissez bien, était justement sur ces thématiques-là. » entretien SHS innovation

En somme, en tant que distribution figée des positions, l'expertise stratifiée est ici œuvre de foi dans les vertus de la pluridisciplinarité<sup>312</sup>, mode de collaboration favorisé par l'organisation en strates et qui place les acteurs dans des positions disciplinaires statiques. Cependant, cette organisation du travail de production va être violemment bousculée par la mise en visibilité croissante du travail jusqu'alors resté invisible.

Cela tient, tout d'abord, de l'aspect dynamique de l'expertise. Dominique Vinck relève sa genèse dans le mouvement critique de la science et sa prise d'autonomie « *autour des modes de décision, de la sociologie des sciences et de la sociologie de l'action collective* » (Vinck, 2007 p. 269) amenant Céline Granjou à accentuer, dans sa définition, l'essence dialogique de l'expertise en réaction aux « *approches participatives* » et aux « *approches gestionnaires* » :

« Les « nouveaux marchés pour la scientification » ouverts par le risque, selon l'analyse d'Ulrich Beck, renvoient alors à des mobilisations en aval des savoirs scientifiques, que l'on distinguera de l'amont de la production scientifique, au sens où il ne s'agit plus de mobiliser des savoirs acquis pour produire de nouveaux savoirs selon les règles de validation propres à une communauté de chercheurs : il s'agit de mobiliser des savoirs théoriques, des compétences et des techniques en réponse à un besoin de maîtrise suscité par des innovations liées à d'autres savoirs. C'est cette forme de médiation mobilisant des savoirs et techniques spécialisés afin de répondre à un besoin de maîtrise des innovations et de leurs possibles conséquences inattendues, que nous désignerons par le terme d'expertise. » (Granjou, 2004 p. 10-11)

---

<sup>312</sup> « D'après J. Piaget (1965, études sociologiques, Droz, Genève), il faut distinguer : la recherche *pluridisciplinaire* dans laquelle plusieurs sciences collaborent chacune conservant sa spécificité ; la recherche *transdisciplinaire* qui se situe à un niveau d'abstraction élevé, utilise des théories et concepts communs à toutes les sciences sociales ; enfin, la recherche *interdisciplinaire*, qui implique la confrontation, échange de méthodes, concepts et points de vue. » (Grawitz, 1996 p. 290-291)

Ce travail<sup>313</sup>, ou plutôt cette position, pour laquelle la médiation est centrale, s'effectue donc sur le pivot de l'incertitude. Elle est d'autant plus prégnante qu'elle se situe dans le champ de l'innovation technologique. Or, si dès les premiers temps de notre association au projet, nous avons pu observer quelques formes de familiarité entre certains partenaires traduisant une interconnaissance antérieure, témoignant d'une habitude à travailler ensemble et accentuant certainement la minoration de l'incertitude dans le projet, loin s'en faut d'en déduire une négligence généralisée de cet élément. Cependant, bien que la tutelle de l'ANR comme organisme financeur conduise à une standardisation des modalités de déroulement et d'organisation des projets concernés qui exclut l'expression claire de l'incertitude sur les résultats à atteindre<sup>314</sup>, lorsqu'elle se manifeste en filigrane, l'incertitude n'est jamais reliée aux positions d'expertise. Donnée comme non problématique dans le descriptif du projet (« taken for granted »), l'expertise est statufiée et consacrée comme autant de briques de l'architecture pluridisciplinaire du projet à édifier. Or, le travail de projection d'usage va ouvrir de larges « *espaces de manœuvre*<sup>315</sup> » internes du seul fait des positions d'expert attribuées à l'origine du projet. Ces espaces de manœuvre vont avoir une action double et d'apparence paradoxale. Ils vont à la fois assurer la sauvegarde des identités professionnelles des acteurs et autoriser une nouvelle économie des rôles attribués initialement dans le projet. En somme, ils sont générés par les caractéristiques consubstantielles à l'expertise :

*« Le rôle de l'expert et le contenu de l'expertise se (re)-construisent au cours de l'action d'expertise. Ils font l'objet d'un apprentissage, d'une appropriation, de négociation entre experts, d'expérimentation et de réflexion avant de se cristalliser dans des cadrages cognitifs communs aux membres du comité. Les experts mettent à l'épreuve leur mandat, construisent une forme de collégialité et une répartition des tâches, découvrent l'incertitude liée à certains savoirs, s'interrogent sur la notion de preuve et développent une conscience des asymétries d'information. Les experts démissionnent de leurs rôles quand le travail*

<sup>313</sup> Notons que la sociologie des professions n'ignore pas l'aspect dynamique de l'expertise : « L'expert se trouve donc souvent en situation de produire une argumentation destinée aux différents acteurs, qu'il s'agisse des commanditaires ou des destinataires de l'expertise. Cette argumentation apparaît tant comme objectif que comme moyen de coordination et d'ajustement. Celle-ci sera destinée à une présentation au public et, sans prétendre à être « vraie », devra se situer dans l'ordre du vraisemblable aux yeux d'un public désormais réputé capable de juger. » (Vrancken, 2004 p. 38)

<sup>314</sup> Nous avons déduit cette information à partir de la lecture d'une vingtaine de projets publics financés par l'ANR depuis 2006 sur le site <http://www.agence-nationale-recherche.fr/>

<sup>315</sup> Cette notion est originellement attachée au caractère à la fois contraignant et habilitant des politiques institutionnelles et des pratiques sur les choix techniques opérés par des chercheurs travaillant sur la détermination du genre de futurs vaccins anti-fertilité : « How then can I describe this "something more" in answering my empirical question about whether and when sex of future users' bodies matters to researchers? In this article, I introduce the notion of the researchers' "room for maneuver." The ability of researchers to generate representations of users and to integrate these into their technical choices is not merely contingent. The range of possibilities can be both enabled and constrained by specific (inter)national or institutional policies and by material practices that have evolved over years of doing reproductive science. » (van Kammen, 1999 p. 310)

*d'expertise ne nourrit pas leurs propres intérêts scientifiques. Ils négocient un partage des rôles entre eux et les décideurs en revendiquant leur scientificité et en se protégeant contre le risque d'usurpation de la légitimité représentationnelle. Ils développent une variété de références à l'incertain, passant par des modalisations spécifiques des énoncés : l'indication des limites de validité des résultats, le recours à des formulations négatives du type « on ne peut pas exclure que... », l'indication d'une absence totale de données et l'expression de certaines divergences entre experts. En fait, ils déplacent le modèle rationnel-légal en prenant en compte les objections apportées par les non spécialistes. Leur compétence vient moins du corpus de savoirs qu'ils maîtrisent que de l'expérience des mécanismes d'objection et d'objectivation à l'œuvre dans leur spécialité, de la récalcitrance du réel et de celle des collègues. » (Vinck, 2007 p. 271)*

Ce projet, qui est au départ mû par cette forme de solidarité organique que constitue la pluridisciplinarité, en se fondant sur le principe d'expertise, sera traversé par les turbulences générées par les différents processus de naturalisation. Or, c'est durant la réalisation de ceux-ci que vont s'ouvrir les espaces de manœuvre à l'intérieur desquels objets et communautés de pratiques vont s'engouffrer. C'est au sein de ces espaces, véritables *imprévus de circonstance*, que va s'élaborer le travail de catégorisation à travers trois phénomènes particulièrement remarquables : la créolisation du langage, la dissémination des capacités réflexives et la génération de *lieux-frontières*, véritables *quasi non-lieux*.

## ***B - Le travail de catégorisation : la convergence de choses***

Le travail de catégorisation (« *categorical work* ») est l'art de jongler avec les « *significations* » qui ont émergé du « *travail d'articulation* » (Bowker & Star, 1999). Ce processus aplanit les écarts de naturalisation et d'appartenance<sup>316</sup>. Cependant, pour Bowker & Star, il ne faut pas se méprendre. La résultante de ce travail n'est pas la « *transparence* » des savoirs, c'est-à-dire le fait que chaque acteur impliqué ait naturalisé complètement l'ensemble des objets et les significations attachées à ceux-ci. Les anthropologues préfèrent parler de phénomène de « *convergence* » : la constitution simultanée d'une personne ou d'un objet et de leurs représentations respectives. Leur insistance à distinguer la « *transparence* » de la « *convergence* » tient du fait que cette dernière ait pour pouvoir d'effacer la traçabilité

<sup>316</sup> « We can see categorical work as partly about managing the mismatches between memberships and naturalization. » (Bowker & Star, 1999)

des catégories préexistantes<sup>317</sup>. Les tensions sont résolues par l'obtention de consensus sur la classification d'un monde à venir (cf. p.181). C'est l'aboutissement d'un processus de déplacements multiples, de *convergence de choses* dont voulons rendre compte dans les lignes suivantes à travers les déplacements convergents observés dans le langage (1), l'expression des réflexivités (2) et enfin dans les lieux et personnes (3).

## 1) Créolisation du langage

Le fait qu'un langage stabilisé, constitutif de chaque position experte, ait été dépassé pour qu'un travail en commun puisse advenir doit être souligné. Jean-Yves Trépos avait déjà suggéré la nécessité de ce dépassement avec le concept d'« *expertise distribuée* » définie comme une « *expertise dont les composantes sont nécessairement incomplètes et en attendent d'autres avant de pouvoir produire un jugement.* » (Trépos, 2001 p. 218). Néanmoins, c'est du côté de la sociologie des sciences que cette incomplétude a trouvé un développement théorique approfondi<sup>318</sup> : Harry M. Collins et Robert Evans, dans leur entreprise de refondation du concept d'expertise, partagent avec le sociologue français l'idée d'une expertise distribuée (« *shared expertise* »), notion qu'ils développent en trois catégories. A chacune de ces catégories d'expertise correspondent des « *zones de marchandage*<sup>319</sup>. » (Galison, 1997 ; Gorman, Groves & Catalano, 2004)

Un premier niveau, l'absence d'expertise distribuée, renvoie à la notion d'incommensurabilité kuhnienne puisque plusieurs paradigmes (ou disciplines ou positions) représentent des visions du monde différentes empêchant leurs porteurs de trouver un espace d'entente. C'est le registre d'expertise que l'on retrouve durant la première phase de scénarisation, la stabilisation de l'intrigue. La zone de marchandage qui y est associée est marquée par le fait que les « *solutions disciplinaires soient balancées par-dessus les cloisons qui maintiennent les disciplines éloignées par un golfe incommensurable*<sup>320</sup>. » Cette zone est donc marquée par une coopération de façade. A titre d'illustration, l'affirmation par le cryptologue de l'inexistence de la notion de Privacy en cryptologie participe de ce

<sup>317</sup> « Where the difference lies between transparency and convergence is that where transparency ideally just produces a reflection of the way things really are (and so, in Jullien's (1995) beautiful phrase captures the "propensity of things" in any situation); convergence can radically break down—over time or across geographical borders. When categories do break down in this fashion they leave no continuous trace back to the previous regime. » (Bowker & Star, 1999)

<sup>318</sup> Bien que nous n'utilisions pas son cadre analytique ici, Paul Carlile propose une approche pragmatique qui mérite d'être citée. (Carlile, 2002)

<sup>319</sup> Ces « trading zones » énoncées par Galison dans son travail sur la collaboration de physiciens et d'ingénieurs dans l'élaboration de radars et de détecteurs de particules sont mises en relation avec chacun des niveaux d'expertise partagée à l'occasion d'un travail sur les conditions pratiques de la convergence NBIC (Gorman, Groves & Catalano, 2004).

<sup>320</sup> « [experts] just throw disciplinary solutions 'over the wall' to other participants across an incommensurable gulf. » (Gorman, Groves & Catalano, p. 59)

principe (**Comité de pilotage 2 (T0+3)**). On pourra également évoquer l'incompréhension de l'équipe Umanlab devant les termes décrivant les types d'attaques possibles durant cette période : « eavesdropping », « skimming » ou encore « attaque en relais ».

Au niveau de l'expertise interactionnelle - « *interactional expertise* », on peut observer des formes de socialisation linguistique « *a minima*<sup>321</sup> » performatives dans le caractère distribué de l'expertise, c'est la théorie de l'incorporation *a minima* - « *minimal embodiment* », résumée ainsi par les auteurs :

*« The social embodiment thesis holds that the particular language developed by any social group is related to the bodily form (or practices) of its members because bodily form affects the things they can do in the world. [...] This is what Wittgenstein seems to be getting at when he said that if a lion could speak we would not understand what it said. He was saying that we would not understand speaking lions because their physical make up is different to ours so the way they cut up the world conceptually – their “conceptual joints”- would be different too. [...] The idea of interactional expertise allows that a single lion with the capacity to speak, if snatched from its cradle and brought up alongside humans in the same way as are domestic dogs and cats, would acquire human language, including the word for chair, even though it, as an individual, could not sit. This is the minimal embodiment thesis. We call it the minimal embodiment thesis because it argues that though bodily form gives rise to the language of a community, only the minimal bodily requirements necessary to learn any language are necessary to learn the language of any community in which the organism is embedded. »* (Collins & Evans, 2007 p. 75)

C'est à ce niveau que la distribution d'expertise s'effectue entre Umanlab et les autres partenaires. En effet, à partir de l'étape de stabilisation de l'instanciation, les partenaires vont faire usage d'un arsenal terminologique qui va structurer leurs échanges : les notions de « Privacy », de « scénario », de « trust », de « confidence », de « sécurité », d'« attaques », de « menaces », d'« usage » vont alors circuler de manière intense. Paradoxalement, cette mise en circulation de notions structurantes va de pair avec le fait que celles-ci soient partiellement vidées de leur substance. En effet, à mesure que la projection d'usage progresse, les notions se défont de leurs ancrages disciplinaires : ceux qui les énoncent ne parlent plus à partir d'un point d'autorité disciplinaire mais s'expriment du territoire de distribution de l'expertise que constitue le projet comme l'illustre cet extrait dans lequel les interlocuteurs rient de la distance prise avec les définitions :

---

<sup>321</sup> Nous détournons ici la traduction de Léa Lima (Lima, 2009).

« Non sans humour, les participants relèvent la gêne que peut provoquer l'homonymie entre scénarios d'attaque et scénarios d'usage, le mot scénario étant indifféremment employé pour les deux :

« **CEA-LETI** – En fait, ça devient difficile parfois de s'y retrouver. (rires)

**Umanlab** – mais, nous sommes bien d'accord, c'est pas la même chose ?

**UVSQ, CEA-LETI** – oui, bien entendu...

**UVSQ** – mais use case et scénario d'usage, c'est synonyme, non ? (rires)

**Umanlab** – oui, enfin, c'est pas la même langue...

**CEA-LETI (chef de projet)** – ça c'est sur, mais bon, faut quand même qu'on parle la même langue pour savoir si on parle de choses différentes (rires). » **Conférence téléphonique (T0 + 7)**

Cette position nouvelle permet ainsi à chacun de pouvoir s'exprimer, compléter ou amender la parole de l'autre sans pour autant en revendiquer l'expertise complète. Au niveau de l'expertise partagée, la zone de marchandage est caractérisée par le développement d'une forme de langage hybride. Nous avons constaté la constitution de cette forme de *créole*<sup>322</sup> comme autre moyen de circonvenir à l'incommensurabilité précitée. Le créole ou pidgin est caractérisé par son caractère auxiliaire et sa forte relation à un contexte particulier, ici, le projet :

*« A pidgin is defined as a stable form of speech that is not learned as a first language (mother tongue) by any of its users, but as an auxiliary language by all ; whose functions are sharply restricted and whose vocabulary and overt structure are sharply reduced, in comparison with those of languages from which they are derived. »* (Hymes, 1968 p. 14)

Durant cette période, le recours de plus en plus fréquent à des « *borrowed artefacts* », en tant qu'éléments de langage objectivés, est symptomatique de cette créolisation, entendue comme :

*« [...] la mise en contact de plusieurs cultures ou au moins de plusieurs éléments de cultures distinctes, dans un endroit du monde avec pour résultante une donnée nouvelle,*

---

<sup>322</sup> « Two groups can agree on rules of exchange even if they ascribe utterly different significance to the objects being exchanged; they may even disagree on the meaning of the exchange process itself. Nonetheless, the trading partners can hammer out a local coordination, despite vast global differences. In an even more sophisticated way, cultures in interaction frequently establish contact languages, systems of discourse that can vary from the most function-specific jargons, through semispecific pidgins, to full-fledged creoles rich enough to support activities as complex as poetry and metalinguistic reflection. » (Galison, 1997 p. 783).

*totalelement imprévisible par rapport à la somme ou à la simple synthèse de ces éléments. »*  
(Glissant, 1997 p. 37)

La scène suivante constitue une illustration éloquente de l'usage de ce créole. Sa lecture est à mettre en relation avec la réaction du responsable de projet Umanlab qui, lors de l'ultime réunion téléphonique (**Conférence téléphonique (T0 + 20)**), nous a demandé si nous avions « capté quelque chose aux discussions techniques et aux différentes sortes de menaces et spécifications » :

« L'intervention du doctorant a ouvert une période de discussion intense essentiellement animée par lui et moi. A partir des plans d'évaluations (contrôle/feedback), nous revenons et discutons la position des points (options techniques) en fonction des explications complémentaires qu'il fournit pour lire le document. La grille permet de mettre en lumière notre mauvaise interprétation de certains protocoles techniques quand elle ne souligne pas l'appropriation de certaines attitudes « sociétales » par Inside. Ainsi, plusieurs dénominations données aux options techniques sur les plans « contrôle/feedback » sont portées à discussion. Au départ, nous avons modifié les appellations originales pour des raisons purement esthétiques, les noms de plusieurs options étant trop long. Cependant, lors de la discussion, nous avons conservé les dénominations courtes, de même que nous avons utilisé les notions de trust et confidence sans avoir à rappeler leurs définitions. Aussi, la notion de configuration d'usage, renvoyant à un quadrant du plan, était complètement assimilée par le doctorant d'Inside ainsi que par le cryptologue de l'UVSQ. Les autres partenaires lui préféraient encore le mot quadrant. Par ailleurs, plutôt que de parler de mode actif ou passif pour le NFC, j'avais adopté le langage du doctorant d'Inside en parlant de mode « écoute » et de mode « initiateur », autre terminologie recouvrant les mêmes fonctions. Le doctorant a également à plusieurs reprises questionné les notions de feedback et de contrôle, puis les a utilisées pour discuter l'exactitude de la position des points. Concernant l'usage de la notion de Privacy, je signale qu'elle est souvent utilisée en lieu et place du mot sécurité dans les parties techniques. Le chef de projet me répond que cela ne nuit pas à l'essentiel puisque « les parties sociétales permettent de mieux comprendre les autres dimensions de la notion ». Enfin, j'ai soulevé une question qui représentait une inconnue pour moi : « Est-ce que l'on doit considérer dans l'ensemble des scénarios que le téléphone mobile est doté d'une fonction d'activation et de désactivation des échanges sans contact ? » Une fois de plus, le doctorant d'Inside m'a répondu en premier : « C'est vrai que c'est l'inconnue orthogonale à l'ensemble des cas que l'on a traité. La question que tu poses en fait, c'est est-ce que le rôle du CPM est de sécuriser juste la carte que contient le



téléphone ou doit-il jouer le rôle de brouilleur ? » Le CEA-LETI, reprenant au vol l'idée de brouilleur, affirme que la question est cruciale pour le projet et qu'elle reste à traiter. »

### **Comité de pilotage 6 (T0 + 17)**

Enfin, le niveau d'expertise distribuée le plus achevé est celui de l'expertise contributive - « *contributing expertise* », distinguant l'expert « *qui comprend* » (ce qui est le cas dans l'expertise interactionnelle) de l'expert « *qui contribue* ». Collins et Evans prennent l'exemple d'une personne qui, par le biais d'un contact régulier avec des plombiers, en arrive à pouvoir dialoguer avec eux et même imaginer des solutions pertinentes (expertise interactionnelle) sans pour autant être à même de changer un joint sur un tuyau (expertise contributive). Dans ce troisième niveau, la zone de marchandage est caractérisée par le partage de concepts et d'applications et ouvre à l'émergence de nouveaux paradigmes. Elle correspond, dans notre cas d'espèce, à un moment auquel nous n'avons pu assister qu'au commencement : l'utilisation de l'infrastructure-frontière, le scénario, comme objet stabilisé. Cet instant marque la mise en sourdine de l'intervention de Umanlab dans le projet et le départ de la phase de conception du CPM.

## **2) Dissémination de l'expression des réflexivités**

Demeure à traiter la question spécifique mais esquissée jusqu'ici des modalités de l'incorporation d'une sociologie praticienne au projet. Au-delà des sources de conflits inhérentes à l'organisation des expertises dans le projet et à ses conséquences pratiques, se pose l'épreuve de la légitimité de ce type d'intervention durant les interactions, la recommandation pressante de l'ANR ne garantissant en rien la fluidité des échanges entre partenaires ni le fait que ceux-ci donnent quittance aux sociologues à la régularité de leurs contributions. Les doutes que nous faisons peser sur le poids relatif qu'a pu avoir la production des sociologues participent bien entendu de la possibilité de voir intervenir un « *boundary work*<sup>323</sup> » de sens commun reléguant les sciences « molles » aux marges de la techno scientificité comme le rappelle ce verbatim :

---

<sup>323</sup> « Boundary-work is an effective ideological style for protecting professional autonomy: public scientists construct a boundary between the production of scientific knowledge and its consumption by non- scientists (engineers, technicians, people in business and government). The goal is immunity from blame for undesirable consequences of non-scientists' consumption of scientific knowledge. » (Gieryn, 1983 p. 789). L'auteur relève à cet égard trois opportunités offrant aux idéologues d'une profession la possibilité de mobiliser ce « boundary work » : lorsque l'objectif poursuivi est l'expansion de l'autorité ou de l'expertise dans des domaines réservés à d'autres professions; lorsque l'objectif est la monopolisation de l'autorité professionnelle et des ressources associées; lorsque l'objectif est la protection de l'autonomie de l'activité professionnelle concernée. Il note que ce type de travail n'est pas limité à la démarcation des sciences des non sciences, mais également utile à la distinction entre disciplines, spécialités ou orientation théoriques à l'intérieur de la science. (Gieryn, 1983 p. 791-792)

« Néanmoins, un des interlocuteurs du CEA-LETI nous apostrophe par une question inattendue : « malgré la qualité du travail, vous n'auriez pas une méthode pour nous dire clairement ce qui va vraiment inquiéter les utilisateurs ? Par exemple, nous dire pour chacun des scénarios quelle serait la meilleure option technique d'un point de vue de l'acceptation sociétale ? » Personnellement échaudé, nous avons répondu que si nous détenions ce type d'informations nous serions déjà riches. De manière surprenante, c'est le doctorant d'Inside qui a coupé court à l'échange en affirmant que « même d'un point de vue strictement technique, il nous est difficile de vraiment décider ce sur quoi nous devons travailler en priorité. » (**Comité de pilotage 6 (T0 + 17)**)

Cette interrogation sur la réception de l'activité SHS et de son produit est d'autant plus fondée que l'on considère le caractère éminemment réflexif des sociétés capitalistes modernes (Beck, 1986 ; Giddens, 1990) :

*« The reflexivity of modern social life consists in the fact that social practices are constantly examined and reformed in the light of incoming information about those very practices, thus constitutively altering their character. [...] In all cultures, social practices are routinely altered in the light of ongoing discoveries which feed into them. But only in the era of modernity is the revision of convention radicalized to apply (in principle) to all aspects of human life, including technological intervention into the material world. It is often said that modernity is marked by an appetite for the new, but this is not perhaps completely accurate. What is characteristic of modernity is not an embracing of the new for its own sake, but the presumption of wholesale reflexivity – which of course includes reflection upon the nature of reflection itself. »* (Giddens, 1990 p. 38-39)

Cette montée en réflexivité trouve un écho dans le recours massif, sinon systématique à la sociologie, sous la forme d'expertise (Trépos, 1996 ; Vrancken & Kutty, 2000 ; Vrancken, 2004), voire comme ressource mobilisée par les acteurs ordinaires (Giddens, 1990 ; Vrancken & Kutty, 2000), ressource à laquelle Giddens reconnaît une valeur supérieure aux autres sciences sociales<sup>324</sup>. Pour l'illustrer, Giddens nous explique que le mariage et la famille ne sauraient être ce qu'ils sont aujourd'hui sans être socialisés ou psychologisés. N'importe quel occidental envisageant de se marier le fait en connaissance du fait que les taux de divorces sont élevés et que cet élément puisse peser sur sa prise de décisions, tout autant qu'il puisse avoir une idée sur les changements des institutions

<sup>324</sup> « In the social sciences, to the unsettled character of all empirically based knowledge we have to add the “subversion” which comes from the reentry of social scientific discourse into the contexts it analyses. The reflection of which the social sciences are the formalized version (a specific genre of expert knowledge) is quite fundamental to the reflexivity of modernity as a whole. [...] All the social sciences participate in this reflexive relation, although sociology has an especially central place. » (Giddens, 1990 p. 40)

familiales, des positions sociales relatives entre hommes et femmes, des mœurs sexuelles, etc. (Giddens, 1990 p. 42-43). Cette réflexivité des savoirs qui engagent les acteurs sur les voies du raisonnement sociologique est « *à forte potentialité déstabilisatrice* » (Vrancken, 2004 p. 39) en ce qu'elle autorise les acteurs non experts, les profanes, à légitimement porter à critique aux catégories savantes<sup>325</sup>. Ainsi, malgré l'étiquetage comme experts dont bénéficie l'équipe SHS au projet, ceux-ci vont trouver leur production discutée par les autres partenaires à mesure que la distribution de l'expertise va s'intensifier. Ainsi, au départ du projet, le respect de l'*expertise stratifiée* limite les incursions dans les domaines d'expertises « étrangers », comme le démontre l'extrait suivant :

« Lors de la réunion avec l'un des membres du CEA-LETI, celui-ci présente l'attaque en relais comme celle sur laquelle les scénarios doivent se concentrer. La priorité, pour le projet, est d'aboutir à l'évaluation des risques. Après avoir fait l'effort de nous expliquer chacune des attaques en des termes plus accessibles, moins techniques, notre interlocuteur admet considérer que les aspects sociaux, économiques et légaux en lien avec la problématique lui sont complètement étrangers. Dès lors, il ne peut apporter son conseil qu'en vertu de critères techniques. Enfin, une discussion s'engage pour savoir en quoi consiste la sociologie et quelles méthodes stables et scientifiques arrivons-nous à développer pour faire de la science. » (**Réunion CEA-LETI/Umanlab (T0 + 4)**)

Néanmoins, d'une part, l'infériorité numérique de l'équipe Umanlab et son intégration tardive au projet<sup>326</sup>, d'autre part, la survenue des différents processus de naturalisation, sont autant de facteurs qui ne favorisent pas non plus le confinement des sociologues dans leur pré-carré disciplinaire. On assiste, à l'inverse, à l'exercice d'un droit de regard sur les productions des sociologues, droit de regard qui s'exerce simultanément par les sociologues envers les productions des technologues. Ainsi, à partir de la stabilisation de l'instanciation, des discussions, souvent bilatérales, vont impliquer les partenaires entre eux. La construction du scénario va s'effectuer par le biais d'un travail critique des uns vers les

<sup>325</sup> « Le fait de poser les questions en axant la réflexion sur d'autres angles du prisme que ceux pratiqués par le commanditaire, le fait d'élargir la commande, d'analyser les logiques, les stratégies et les tactiques des acteurs en présence, font que l'intervenant sociologique participe à une production de connaissance qui nourrit à la fois les représentations des sujets et les orientations de l'action. De plus, et parce que, comme nous l'avons vu, la demande sociale exige désormais le croisement de savoirs pluriels, les apports du sociologue sont complémentaires à ceux des professionnels issus d'une autre formation et maîtres d'œuvre d'une autre pratique d'intervention. Cette plus value est donc nécessairement insuffisante en elle-même mais singulière et donc riche d'enseignement pour la gestion des problèmes à traiter. » (Legrand, 2004 p. 100)

<sup>326</sup> Pinch considère que dans les situations de conception fondée sur des interactions fortes entre groupes sociaux, trois sortes de configurations peuvent être distinguées : l'une dans laquelle il n'y a pas de groupes dominant, la seconde pour laquelle un groupe dominant peut imposer sa propre définition de la situation et pour la troisième, plusieurs groupes aux forces égales s'affrontent (Pinch, 1993 p. 128-129). En vertu du règne de l'enthousiasme technologique, l'on peut penser que nous nous trouvons dans la deuxième situation qui favorise l'expression des partenaires techniques. Néanmoins, le processus de *technologisation* de l'intrigue permet aux sociologues de rétablir le rapport de forces en abordant les problèmes « sociaux » par le versant technologique. Ici, notre cas d'espèce oscillerait entre la première et la dernière situation.

autres, par des aller-retour enrichissant les productions intermédiaires. Cette *fertilisation croisée* s'effectue grâce au développement d'une critique réflexive collective qui ignore, au moins jusqu'au niveau de l'expertise interactionnelle, les pré-requis disciplinaires ou statutaires nécessaires au droit de cité. La légitimité à s'exprimer est fondée par la participation au projet et au degré de naturalisation des artefacts en conception. Ce passage synthétise cet état de fait :

« Durant le trajet, l'un des membres du CEA-LETI, parcourant le document fourni par Inside et UVSQ, se tourne vers nous et nous demande une précision technique sur l'un des cas décrits. Une discussion d'un quart d'heure s'est alors engagée sur la lecture et la compréhension des autres cas entre membres du CEA-LETI et l'équipe Umanlab (à noter l'absence du responsable projet). » (**Comité de pilotage 6 (T0 + 17)**)

Les phénomènes de créolisation du langage et de dissémination de l'expression des réflexivités renseignent sur le déploiement du savoir produit. Celui-ci circule, durant le temps de la projection d'usage, au sein d'une zone de validité circonscrite aux frontières du projet. Ainsi, les participants au projet en sont autant les producteurs que le réceptacle. Tandis que l'expertise stratifiée constituait le reflet d'une écologie de lieux à partir desquels se fondent les jugements, les frontières établies par cette géographie du bien-fondé à s'exprimer sont brouillées par l'établissement de ce « *cycle de crédibilité*<sup>327</sup> » étanche que constitue le projet. Il n'est dès lors plus possible pour les acteurs de ne faire appel qu'à leurs positions d'expert pour être entendus<sup>328</sup> car celles-ci sont diluées par la dynamique de projection d'usage. Le sujet tend ainsi à s'effacer, à se fondre dans les processus et ses productions associées<sup>329</sup>.

Ainsi, la dissémination de l'expression des réflexivités participe d'un *ancrage ultra-local de circulation du savoir produit*. Ce constat amène la reconnaissance du coût élevé du transfert de ce savoir à l'extérieur de sa zone de production, ou plus précisément vers d'autres acteurs que ces producteurs-récepteurs. C'est un savoir fortement « *englué*<sup>330</sup> » (von Hippel, 1994) dont le transfert nécessiterait d'intenses efforts de traduction formelle. C'est

<sup>327</sup> (Latour & Woolgar, 1979 ; Rip, 1994)

<sup>328</sup> « Listening is active, not passive; it means stretching to affiliate with multiplicity. » (Bowker & Star, 1999 p. 308)

<sup>329</sup> C'est ce que Wagner nomme, en prenant une position particulièrement normative, la distinction sujet/processus : « Exploring the "subject-process" distinction seems a fruitful route to some of the problems of multidisciplinary work. While sense making is indispensable for developing an understanding of what "provokes" actors to modify, re-initiate, justify, hide, and manipulate, a process-oriented perspective offers some common ground for learning what helps to ensure the ongoing flow of communication and cooperation within a field. » (Wagner, 1997 p. 429)

<sup>330</sup> « We define the stickiness of a given unit of information in a given instance as the incremental expenditure required to transfer that unit of information to a specified locus in a form usable by a given information seeker. When this cost is low, information stickiness is low; when it is high, stickiness is high. Note that in our definition, information stickiness involves not only attributes of the information itself, but attributes of and choices made by information seekers and information providers. » (von Hippel, 1994 p. 432)

un investissement de forme dont le retour ne peut être évalué simplement. En effet, si la catégorisation s'effectue par une succession de stabilisations<sup>331</sup>, en l'espèce l'homogénéisation des sens attribués au scénario par la constitution d'une infrastructure-frontière, la fin de la projection ne marque que le début du processus de fermeture des incertitudes, de résolution d'un problème, voire d'une controverse<sup>332</sup>.

### 3) Borderlands et Lieux-frontières

Enfin, nous avons également noté que ce travail de catégorisation, mis en visibilité par la créolisation du langage et la dissémination de l'expression des réflexivités, s'effectuait souvent en des endroits réservés. En effet, une large partie du travail de catégorisation a pris place durant les réunions téléphoniques, pendant les déjeuners, les discussions informelles, durant les trajets en voiture, dans les couloirs, dans tous ces lieux où personne n'assume de travail de secrétariat, ces lieux sans compte-rendu, c'est-à-dire sans comptes à rendre. Nous avons identifié ces endroits comme des *quasi « non-lieux »* en ce qu'ils en partagent l'essence bien qu'ils s'en démarquent par certaines caractéristiques. Marc Augé (1992) leur accorde une définition négative relative à celle du lieu anthropologique :

*« Si un lieu qui peut se définir comme identitaire, relationnel et historique, un espace qui ne peut se définir ni comme identitaire, ni comme relationnel, ni comme historique définira un non-lieu. En effet, ils se rapprochent du concept en ce qu'ils ne se définissent pas a priori sur des critères identitaires, relationnels ou historiques. »* (Augé, 1992 p. 101)

Ainsi, ces lieux d'élaboration du travail d'articulation ont en partage certains attributs typiques de ces « *non-lieux* ». Ils sont effectivement des endroits de passage où le travail est présenté comme fugace et temporaire, du moins lorsqu'il n'en est pas explicitement exclu<sup>333</sup>. Cependant, ils s'en distinguent sur la manière dont ils exercent leur performativité.

D'abord, la médiation de ces « *non-lieux* » s'effectue par des artefacts (textes, mots, OIC). Ces lieux « *n'existent que par les mots qui les évoquent, non-lieux en ce sens ou plutôt lieux imaginaires, utopies banales, clichés.* » (p. 120) Ils sont tributaires d'une médiation qui passe par les mots et les textes. Or, la particularité des *quasi « non-lieux »* tient à leur

<sup>331</sup> « The more homogeneous the meanings attributed to the artifact, the higher is the degree of stabilization. » (Pinch, 1993 p. 121).

<sup>332</sup> Ce concept est originellement apparu dans le domaine de la sociologie de la connaissance scientifique et désignait la fin d'une controverse par l'émergence d'un consensus au sein d'une communauté scientifique donnée. Cette fermeture de l'incertitude provoque irrémédiablement une réécriture de l'histoire, l'extinction de toute flexibilité interprétative et le règne des explications monocausales.

<sup>333</sup> « Un monde où l'on naît en clinique et où l'on meurt à l'hôpital, où se multiplient, en des modalités luxueuses ou inhumaines, les points de transit et les occupations provisoires [...] » (Augé, 1992 p. 100)

*ultraperformativité*. En définissant les « *non-lieux* », Marc Augé relève qu'ils décrivent deux réalités complémentaires et distinctes. Ce sont « *des espaces constitués en rapport à certaines fins (transport, transit, commerce, loisir), et le rapport que des individus entretiennent avec ces espaces. Si les deux rapports se recouvrent assez largement, et, en tout cas, officiellement (les individus voyagent, achètent, se reposent), ils ne se confondent pas pour autant car les non-lieux médiatisent tout un ensemble de rapports à soi et aux autres qui ne tiennent qu'indirectement à leurs fins.* » (Augé, 1992 p. 120) Cette distinction, qui renvoie à la définition de Michel de Certeau de l'espace comme « *lieu pratiqué* », se désagrège durant le processus de scénarisation. En effet, dans ces interstices que sont les *quasi* « *non-lieux* », l'espace et le « (non)-lieu » s'agrègent car le lieu ne préexiste plus à l'espace : il surgit lors de sa pratique, il n'est plus distinguable de l'espace. Autrement dit, la projection d'usage et ses versions intermédiaires, créent l'espace et le lieu de leurs pratiques de conception.

D'autre part, et de manière liée, ces « *non-lieux* » produisent un acteur moyen, acteur aux spécificités gommées par sa présence-même dans le « *non-lieu* ». Cet acteur se définit alors avant tout par sa qualité d'utilisateur<sup>334</sup> du « *non-lieu* ». L'idée de moyenne pouvant charrier une dénotation négative, nous lui associons ici moins cette faculté de « *n'être et de ne faire pas plus ni moins que ce que les autres sont et font* », mais plutôt l'idée d'être en capacité d'être et de faire ce que d'autres peuvent être et faire. En cela, l'on peut affirmer que nos *quasi* « *non-lieux* » constituent un lieu d'expression privilégiée de l'ingénierie hétérogène<sup>335</sup>. Ils gomment les positions sociales établies pour favoriser l'émergence d'une identité collective<sup>336</sup>.

Or, le bridage de la qualification de ces lieux en « *non-lieux* » purs<sup>337</sup> est ici aussi justifié. Car, Marc Augé souligne le fait que les lieux se caractérisent par la création de « *social organique* », à l'inverse des « *non-lieux* », qui créent de la « *contractualité solitaire* ». Cet accent mis sur l'individualisation du rapport au lieu s'oppose sensiblement à nos observations pour lesquelles nous n'avons pu constater ni d'émancipation des figures

<sup>334</sup> « Toutes les interpellations qui émanent de nos routes, de nos centres commerciaux ou des avant-gardes du système bancaire au coin de nos rues visent simultanément, indifféremment, chacun d'entre nous (« Merci de votre visite », « Bon voyage », « Merci de votre confiance »), n'importe lequel d'entre nous : elles fabriquent « l'homme moyen », défini comme utilisateur du système routier, commercial ou bancaire. » (Augé, 1992 p. 126)

<sup>335</sup> « To efface this oscillation between singularity and multiplicity, to imagine heterogeneity simply form a control or engineering point of view is, then, [...] a cultural bias. [...] The notion of "heterogeneous engineering" [...] may be treated as a way of thinking about oscillation, absence/presence, uncertainty, and the necessary Otherness that comes with the project of centering. In short, it may be treated as a feature or an aspect of complexity [...] » (Law & Mol, 2002 p. 136-137)

<sup>336</sup> « Alors que c'est l'identité des uns et des autres qui faisait le 'lieu anthropologique', à travers les connivences du langage, les repères du paysage, les règles non formulées du savoir-vivre, c'est le non-lieu qui crée de l'identité partagée des passagers, de la clientèle ou des conducteurs du dimanche. » (Augé, 1992, p. 127)

<sup>337</sup> Notons que Marc Augé convoque ce concept en soulignant son caractère idéal-typique et considère, en conséquence, non-lieu et lieu comme « des polarités fuyantes. » (Augé, 1992 p. 101)

individuelles, ni de formes d'anomie organisée, du moins jusqu'au déclenchement des processus de naturalisation. Au contraire, la contractualité observée est *collégiale*.

Ainsi, les fréquents rappels à l'existence du contrat (notamment par l'évocation permanente des « *structuring artefacts* »), caractéristiques des « *non-lieux* », sont adressés à l'ensemble du collectif sinon aux communautés de pratiques impliquées mais jamais directement aux individus. En ce sens, contrairement à ce qu'affirme Marc Augé, le contrat a toujours rapport avec l'identité collective<sup>338</sup> de celui qui y souscrit. Plus loin, la formation de cette identité collective est notamment transcendée par la circulation d'individus particuliers au sein de ces *quasi* « *non-lieux* » : les « *borderlands* ».

A la base, ce sont des individus appartenant à plusieurs communautés de pratique. Dans notre cas, leur « *marginalité*<sup>339</sup> » s'exprime durant leurs déplacements dans les *quasi* « *non-lieux* ». Parce qu'ils y rejettent l'exclusivité d'affiliation à une seule communauté de pratique, ils transforment ces *quasi* « *non-lieux* » en *lieux-frontières* du seul fait, non de leurs présences, mais de leurs déplacements à l'intérieur de ceux-ci. Le *lieu-frontière* est un *quasi* « *non-lieu* » pratiqué.

Dans le projet COPRIM, le doctorant d'Inside est l'exemple idoine d'un de ces pratiquants en ce qu'il s'est autorisé des incursions dans des champs disciplinaires non familiers tout en autorisant que d'autres (notamment moi) puissent discuter ses contributions cryptologiques.

Enfin, Marc Augé (Augé, 1992 p. 144) identifie dans l'intersection des lieux et des « *non-lieux* » un « *point d'achoppement* » qui « *sera toujours politique.* » Or, en parlant de *quasi non-lieux* pour évoquer les endroits où retentit le plus le travail de catégorisation, nous inscrivons ceux-ci dans un espace avant-coureur du politique. Par cette formule, nous nous référons au mot de Bruno Latour (2005) qui, faisant sien l'aphorisme de Clausewitz, pense la science comme continuation de la politique par d'autres moyens. Non pas que nous voulions affirmer que ce qui permet de remettre les choses en place (« *work that gets things back on track in the face of the unexpected* » (Bowker & Star, 1999 p. 310) et que le travail de catégorisation soient a-politique ou a-scientifique. La piste que nous empruntons ici vise à rappeler que la substitution de l'expertise distribuée à l'expertise stratifiée ainsi que la paradoxale visibilité du travail d'articulation rapprochent sensiblement celui-ci du

---

<sup>338</sup> « identité individuelle » chez Augé, p.128

<sup>339</sup> « Marginality as a technical term in sociology refers to human membership in more than one community of practice [...] Marginality is an interesting paradoxical concept for people and things. On the one hand, membership means the naturalization of objects that mediate action. On the other, everyone is a member of multiple communities of practice. » (Bowker & Star, 1999 p. 302)

« *production work* ». Si le travail de projection d'usage participe de la science, pour que science puisse être produite, il faut qu'une mise à distance soit effectuée entre la science telle qu'elle se fait et la science telle qu'elle s'objective. Or, la projection n'est que formalisation primitive du travail de catégorisation. Elle ne fait pas frontière entre ce qui fait science et ce qui ne fait pas science, mais entre ce qui sera *fait sens* ou non dans le projet – le *vraisemblable*. Elle s'effectue donc antérieurement au « *boundary-work*<sup>340</sup> » : elle est l'infrastructure-frontière qui l'autorise. Elle est, en ce sens, *pro-politique* car elle y est à la fois antérieure et favorable.

### C - La composition d'axiomes

En se penchant sur la projection d'usage, se sont dévoilées des dynamiques des carrières, de fiction et de scénarisation. Au sein de ces mouvements, sont pêle-mêle mis à plat la chaîne hiérarchique entre la science, la technologie et le sens commun<sup>341</sup>, la distinction entre science et sens commun ou entre *anima* et *animus*, le *distinguo* entre le réel et l'inventé, la stratification de l'expertise, l'étanchéité des champs de connaissances et les obstacles épistémologiques bachelardiens. Cette dernière référence sert ici moins à s'aventurer sur les chemins tortueux de l'épistémologie qu'à proposer une piste de réflexion sur l'inscription de la projection d'usage au sein d'un mouvement plus général, celui que Gilbert Durand (1988) nomme l'« *après-Bachelard* » :

« *L'après-Bachelard* » serait donc ce moment historique et culturel dans lequel les deux modalités du savoir – sans toutefois se confondre puisqu'en dernier ressort c'est la spécificités du point d'application qui décide des méthodes – convergent en une philosophie d'ensemble, dans de « nouvelles formes a priori » non Kantienne, dans une temporalisation des phénomènes non hégélienne, dans des définitions d'objets non comtiennes, dans des rapports dialectiques non marxien, et finalement dans des logiques délibérément non aristotéliennes. » (Durand, 1988, 9)

<sup>340</sup> « Boundary-work is an effective ideological style for protecting professional autonomy: public scientists construct a boundary between the production of scientific knowledge and its consumption by non-scientists (engineers, technicians, people in business and government). The goal is immunity from blame for undesirable consequences of non-scientists' consumption of scientific knowledge. » (Gieryn 1983: 789). L'auteur relève à cet égard trois opportunités offrant aux idéologues d'une profession la possibilité de mobiliser ce « boundary work » : lorsque l'objectif poursuivi est l'expansion de l'autorité ou de l'expertise dans des domaines réservés à d'autres professions ; lorsque l'objectif est la monopolisation de l'autorité professionnelle et des ressources associées ; lorsque l'objectif est la protection de l'autonomie de l'activité professionnelle concernée. Il note que ce type de travail n'est pas limité à la démarcation des sciences des non sciences, mais également utile à la distinction entre disciplines, spécialités ou orientation théoriques à l'intérieur de la science. (Gieryn 1983: 791-92)

<sup>341</sup> On fait ici référence aux déterminismes techniques dont on trouve la synthèse dans le slogan de l'exposition universelle de 1933 à Chicago « A Century of Progress ». Sa devise était alors « Science Finds, Industry Applies, Man conforms. »



Poser cela, c'est certainement refuser de trancher entre le constat d'une non-modernité idéal-typique (Latour, 1991) ou celui d'une postmodernité exaltée (Maffesoli, 2000). En effet, notre analyse emprunte aux deux constats : l'effort d'analyse symétrique entre humain et non-humain coexiste avec le constat d'un enthousiasme technologique pour le moins moderne. Ce qui nous intéresse dans l'inscription de ces mouvements, c'est notamment la remise en cause de l'opposition opérée par Bachelard entre science et poésie<sup>342</sup>. Durand mobilise son savoir encyclopédique<sup>343</sup> pour mettre à jour les indices de cette convergence. L'hypothèse scientifique y naît d'une subjectivité thématique et elle renverse les cadres explicatifs établis :

*« Disons simplement qu'apparaît à l'horizon des procédures nouvelles d'explication, et en conformité totale avec les notions de « forme causative/chréode/bassin sémantique », la notion paradoxale d'effet causatif c'est-à-dire de phénomènes qui rétroactivement déterminent (ou « choisissent ») leurs séries causales de rattachement. »* (Durand, 1988, 11)

La projection d'usage participe de ces procédures d'explication nouvelle en ce qu'elle cristallise des savoir-être et des savoir-faire multiples dans des *axiomes*. Ces *axiomes* ont eux-mêmes vocation à produire un « effet causatif » : rétroactivement leur action se doit d'être inscrite dans la trajectoire de production de l'œuvre scientifique, d'où l'impératif de vraisemblance.

L'analyse de cette pratique de la recherche n'est pas un discours sur la méthode. Bien sûr, on a pu observer la mise en place d'outils, de méthodes, de techniques de réduction du risque d'incertitude. Néanmoins, mettre l'accent sur la construction d'un *axiome* relève intrinsèquement d'un paradoxe fort : car l'*axiome* est indémontrable. Notre entreprise analytique relève de la description des « *Method Assemblage*<sup>344</sup> » (Law, 2004). Inspiré par la notion d'agencement<sup>345</sup> développée par Deleuze et Guattari (Deleuze & Guattari, 1980) et

<sup>342</sup> « Pour Bachelard, nous le savons « les axes de la poésie et de la science sont inverses », « l'attitude scientifique consiste précisément à résister contre l'envahissement des symboles », ou encore : « Le concept scientifique fonctionne d'autant mieux qu'il est sevré de toute arrière image... » Donc une sorte de renforcement extrême des positions du rationalisme scientifique qu'exprime la nécessité de faire subir une « psychanalyse objective » à tout concept scientifique afin de purifier ce dernier de tout retentissement affectif, de toute école buissonnière de la rêverie. » (Durand, 1988 p. 8)

<sup>343</sup> Savoir qui s'aventure autant sur le terrain vaste des sciences sociales que sur celui des sciences dites « dures ». Durand convoque ainsi plusieurs notions qui lui semblent témoigner de cette convergence : la *thema* et les *themas* de Gerald Holton, la phase de la représentation de Sorokin, les schèmes verbaux et mythologèmes de Durand, le travail d'Henry Corbin avec la notion d'*alam al mithal*, récit visionnaire organisateur ou encore l'*unus mundus* jungien. Côté sciences dures, il mobilise notamment le travail du physicien David Bohm et de celui du biologiste Sheldrake.

<sup>344</sup> Sur les difficultés de traduction de la notion d'agencement par celle d'assemblage, on pourra se reporter à l'analyse de John Phillips. (Phillips, 2006)

<sup>345</sup> « En aucun cas nous ne prétendons au titre d'une science. Nous ne connaissons pas plus de scientificité que d'idéologie, mais seulement des agencements. Et il n'y a que des agencements machiniques de désir, comme des agencements collectifs d'énonciation. Pas de signifiante, et pas de subjectivation : écrire à *n* (toute énonciation individuée reste prisonnière des significations dominantes, tout désir signifiant renvoie à des sujets dominés). Un agencement dans sa multiplicité travaille à la fois forcément sur des flux sémiotiques, des flux matériels et des flux sociaux (indépendamment de la reprise qui peut en être faite dans un corpus théorique ou scientifique). On n'a plus une tripartition entre un champ de réalité, le monde, un

ses déplacements d'identités et de territoires, le sociologue britannique en isole quatre caractéristiques majeures :

- l'alliance entre un épistémê et des technologies
- son caractère contingent et *ad hoc* relatif à l'assemblage de composants incompatibles
- sa capacité à embrasser des pratiques mouvantes et dynamiques
- et l'absence de règles générales à suivre pour obtenir de « bons » agencement.

Pour Law, la pratique de la science est constitutive de la science elle-même. Autrement dit, la production et la description de la réalité scientifique sont deux phénomènes concomitants. Pour appréhender ce constat autrement qu'un plaidoyer pour le tout-constructivisme, il faut revenir aux enseignements de la sociologie des sciences et des techniques. La science n'est pas la conquête d'une réalité universelle qui existerait « en-dehors » du champ de connaissance contemporain. La réalité décrite et construite par la pratique scientifique est d'abord la résultante d'un choix entre plusieurs possibles. L'éventail des possibles ainsi que le choix effectué dépendent largement du potentiel d'intéressement de la recherche<sup>346</sup>. Le fait d'être conscient qu'un choix s'opère dans le choix du « dehors » permet de penser la pertinence des réalités à mettre en avant et des rapports d'intérêts et du potentiel d'intéressement. Ce qui implique une rencontre, un échange, des négociations entre les réalités « en-dehors<sup>347</sup> » et les pratiques « en-dedans ». Celles-ci sont, par ailleurs, fortement structurées par des *hinterlands* constitués de sentiers de dépendance de pratiques, des réseaux d'acteurs, des instruments, des politiques de financement, du matériel, etc. En termes de vocabulaire, la notion de « méthode » souffre cependant de ne rendre fidèlement compte ni de l'étendue de ces *hinterlands*, ni des pratiques d'agencement à l'œuvre.

Le néologisme de « *method assemblage* » vise à pallier cette défaillance. Pour Law, l'objectif de création de nouvelles réalités « en-dehors » et de nouveaux savoirs sur ces réalités « en-dedans » implique nécessairement la conception et la valorisation de pratiques à même de *faire avec l'hinterland* des réalités matérielles et sociales préexistantes. L'agencement de méthodes est la mise en œuvre de cet *hinterland* et de son faisceau de

---

champ de représentation, le livre, et un champ de subjectivité, l'auteur. Mais un agencement met en connexion certaines multiplicités prises dans chacun de ces ordres, si bien qu'un livre n'a pas sa suite dans le livre suivant, ni son objet dans le monde, ni son sujet dans un ou plusieurs auteurs. Bref, il nous semble que l'écriture ne se fera jamais au nom d'un dehors. Le dehors n'a pas d'image, ni de signification, ni de subjectivité. Le livre, agencement avec le dehors, contre le livre-image du monde. Un livre-rhizome, et non plus dichotome, pivotant ou fasciculé. » (Deleuze & Guattari, 1980 p. 32-33)

<sup>346</sup> voir chapitre IX.B

<sup>347</sup> Pour Law, cet en-dehors peut prendre deux formes : soit il se manifeste par son absence manifeste dans l'en-dedans, soit il se manifeste par une altérité indéfinie, nécessaire mais fuyante (cf. notre utilisateur).

relations ramifiées. L'agencement participe d'hinterlands variés tout en générant les siens propres qui changent de formes tout en se maintenant dans un territoire tacite, impur et indéterminé<sup>348</sup>, comme nos *axiomes*. Ces assemblages de méthodes, en combinant l'en-dedans et certains en-dehors, jouent également les rôles de détecteurs de réalité et d'amplificateurs du réel.

On retrouve, entre notre analyse de la projection d'usage et l'outillage offert par le « *method assemblage* » de nombreux points de convergence. L'interdépendance du mouvement (l'action de projeter l'usage) et de son résultat (la projection d'usage ou l'axiome fictionnel), l'alliance entre un épistèmê (l'enthousiasme technologique) et des technologies (techniques, représentations, données), son caractère ultra-local et contingent ou encore les flux d'identités et de pratiques. Ce constant bouscule la dernière mouture de la définition adoptée de la projection d'usage, la *représentation de fictions axiomatiques au service de la recherche technologique*. En effet, réduire la projection à l'acte de représentation fait écho aux insuffisances contenues dans la notion de méthode. Notre analyse demande un enrichissement ultime.

Le dernier chapitre de ce travail a pour titre « la composition d'axiomes ». Le choix du terme *composition* s'inscrit dans l'optique du travail de Law tout en visant à se débarrasser des connotations dommageables de la notion de méthode.

La composition désigne à la fois l'action de composer et le résultat de cette action. Cette notion a fait l'objet d'une étude approfondie dans le champ de la sémiologie musicale (Nattiez, 1987) qui a notamment permis la distinction de trois niveaux d'analyse bien distincts : la *poïesis* – niveau de la création, l'*esthesis* – niveau de la réception et le niveau *neutre*, correspondant à la partition. En nous appuyant sur cette analyse, nous distinguons donc une triade de significations rattachées à la notion de *composition*.

Au niveau de la poïesis, composer renvoie au fait de poser ensemble, placer ensemble, faire un tout à l'aide d'éléments, accorder, mettre en ordre, régler un différent, convenir de quelque chose. Composer, c'est donc d'une part, négocier la diversité et l'altérité à potentiel conflictuel à travers la création d'un nouvel ordre vraisemblable. La composition permet donc de faire et d'être avec l'autre ce qu'il n'était pas possible de faire ou d'être sans lui. C'est faire ensemble. Composer, c'est d'autre part faire avec, dans le sens de s'accommoder de l'absence, la déjouer. Malgré la proximité évidente avec l'univers notionnel du

---

<sup>348</sup> « 'method assemblage' grows out of but also creates its hinterlands which shift in shape as well as being largely tacit, unclear and impure. » (Law, 2004 p. 42)

bricolage<sup>349</sup>, il faut se garder de tout rapprochement hâtif, car il y a dans la notion de bricolage le présupposé d'une action hors du territoire de la science<sup>350</sup>. Si la sociologie des sciences a déjà abordé ces questions, la substitution de la *composition* à la *représentation* rend notamment compte du caractère sibyllin de la projection d'usage.

Le niveau de l'*esthesis* n'a pas été pleinement abordé dans notre travail. Il mériterait une étude à lui seul. La circulation de la projection en dehors du cercle de ses créateurs n'a été abordée qu'à l'intérieur du cercle de diffusion commanditaires-équipe-projet. Cependant, un lien clair est établi entre l'*axiome* et sa réception. En préparant les qualités axiomatiques de la projection, ces *compositeurs* que constitue l'équipe projet dépossèdent le récepteur de toute tentative de démontage de la *vraisemblance* de cette projection. Les tests qui vont être effectués durant la suite du projet sont des tests d'ajustements (Anjembe & Verchère, 2010 ; Verchère & Anjembe, 2010) du niveau de la *vraisemblance*. Ils ne visent en aucun cas à s'imposer comme des remises en questions brutales du niveau de réel présumé. En tout état de cause, c'est comme cela que le voient les concepteurs.

Le niveau neutre correspond, dans notre cas d'espèce, à l'*axiome* en soi, la partition qui matérialise la projection d'usage. L'*axiome* est issu d'un acte de création, nécessairement innovant, parce qu'il est cristallisation d'une assemblée de « *porte-paroles* » *vraisemblables*<sup>351</sup> s'exprimant au nom d'un peuple d'actants variés mais agissant sur l'ordre d'un acteur unique : l'équipe-projet. Dans l'*axiome* est annihilée l'historicité des parcours et

<sup>349</sup> Pour plus de détails, on peut se référer à (Knorr, 1979 ; Clarke, A. & Fujimura, 1992 ; Nutch, 1996 ; Vinck, 2003)

<sup>350</sup> « Le bricoleur est apte à exécuter un grand nombre de tâche diversifiées; mais, à la différence de l'ingénieur, il ne subordonne pas chacune d'elles à l'obtention de matières premières et d'outils, conçus et procurés à la mesure de son projet : son univers instrumental est clos, et la règle de son enjeu est de toujours s'arranger avec les " moyens du bord ", c'est-à-dire un ensemble à chaque instant fini d'outils et de matériaux, hétéroclites au surplus, parce que la composition de l'ensemble n'est pas en rapport avec le projet du moment, ni d'ailleurs avec aucun projet particulier, mais est le résultat contingent de toutes les occasions qui se sont présentées de renouveler ou d'enrichir le stock, ou de l'entretenir avec les résidus de constructions et de destruction antérieures. L'ensemble des moyens du bricoleur n'est donc pas définissable par un projet (ce qui supposerait d'ailleurs, comme chez l'ingénieur, l'existence d'autant d'ensembles instrumentaux que de genres de projets, au moins en théorie); il se définit seulement par son instrumentalité, autrement dit et pour employer le langage même du bricoleur, parce que les éléments sont recueillis ou conservés en vertu du principe que " ça peut toujours servir ". De tels éléments sont donc à demi particularisés: suffisamment pour que le bricoleur n'ait pas besoin de l'équipement et du savoir de tous les corps d'état mais pas assez pour que chaque élément soit astreint à un emploi précis et déterminé. Chaque élément représente un ensemble de relations, à la fois concrètes et virtuelles; ce sont des opérateurs, mais utilisables en vue d'opérations quelconques au sein d'un type. » « la Pensée sauvage », Paris, Ed. Plon, 1960, p 27.

<sup>351</sup> « L'innovation est faite de décisions, mais de décisions d'un type particulier. Elles tournent toutes autour d'une même et seule interrogation : cette suggestion qui m'est faite, ce résultat dont on me demande de tenir compte, cette information que me donne ce spécialiste du marketing, ce comportement nouveau des électrons que décrit un article récemment publié, ces assurances que me donne le maire de New York, tout cela mérite-t-il d'être cru ? En d'autres termes, en prenant les décisions qu'appellent ces recommandations ou ces réactions, vais-je augmenter le nombre de ceux qui me soutiennent ? Les usagers, les électrons, les concurrents, les banquiers vont-ils vraiment agir comme l'affirment tous ces porte-parole qui m'entourent et dont je ne sais pas vraiment s'ils sont représentatifs, c'est-à-dire s'ils ne vont pas être démentis dans les instants suivants par tous ceux, électrons, consommateurs, banquiers, au nom desquels ils prétendent parler. Voilà où gît l'incertitude. L'innovateur qui réussit est celui qui arrive à la maîtriser en choisissant les bons interlocuteurs. Choix stratégique qui dépend du projet en cours mais qui suppose aussi cette irremplaçable intuition qui fait que dans certains cas on a l'impression qu'un faisceau de présomptions qui rendent crédible ce discours singulier tenu par un être unique. Ce n'est qu'après coup, mais après coup seulement, que l'on saura sans ambiguïté si les porte-parole retenus étaient légitimes. » (Akrich, Callon & Latour, 1991 p. 68-69)

des décisions individuelles au profit d'une partition sans dissonances<sup>352</sup>. La critique de cet *axiome* ne peut être qu'une mise en cause de son caractère *vraisemblable*, c'est-à-dire un mode de jugement portant sur la capacité de l'*axiome* à répondre aux attentes du public auquel il est exposé. En tant que tel, dans un absolu et si l'absolu existait, cet axiome n'aurait aucune raison d'être car il n'a de fondement que dans ses capacités attendues d'attacher, d' enrôler, d'intéresser d'autres choses ou d'autres êtres.

Cette raison d'être de l'*axiome* nous permet d'aborder la question de la raison d'agir. Il ressort de notre analyse l'évitement de toute tentation d'emprunter un chemin normatif visant à définir un guide des bonnes pratiques de la projection d'usage. On se doit néanmoins de faire l'aveu de l'existence d'un arrière-plan, d'un *hinterland* qui nous est propre. Conformément à notre engagement introductif, les unités découpées sont des « *composites qui articulent des situations, des objets et des discours* » (Le Marec, 2002 ; Le Marec & Babou, 2003). Ces trois objets ont impliqué notre personne. Nous avons taché de faire en sorte que notre voix ne puisse primer sur celle des composites qu'elle a évoqués (Woolgar, 1991) : la composition de la projection s'est bien construite dans notre relation à l'objet crée et étudié. Or, cette construction s'est faite avec, en arrière-plan l'intime conviction que la sociologie pouvait encore être utile aux contacts d'acteurs considérés compétents. La morale et l'éthique, à laquelle nous avons feint de ne jamais vouloir nous approcher au départ, reviennent en force avec cette question clé : A qui s'attacher ? En effet, le choix du terme réside aussi dans le fait que composer, c'est accomplir un acte politique.

Si l'attachement est jugé d'emblée absolument nécessaire à l'accomplissement de la projection, la question qui s'impose de manière péremptoire est alors : « *comment choisir les acteurs avec qui l'on travaille ?* » (Callon, 1999). Avec Callon, nous abondons dans le sens qu'il faille privilégier les acteurs qui ont un fort degré d'innovation car les problèmes qu'ils se posent font émerger de nouvelles questions et de nouvelles pratiques, et qu'ils créent des asymétries entre acteurs en dotant (ou en ôtant) à certains d'entre eux la parole dans le processus d'élaboration de l'innovation.

Dans l'univers empirique dans lequel nous nous sommes plongés, la partie n'est pas aisée<sup>353</sup> quand elle n'est pas tout simplement méprisée. Mais les questions soulevées par notre

---

<sup>352</sup> « Le storytelling est donc une opération plus complexe qu'on ne pourrait le croire à première vue : il ne s'agit pas seulement de « raconter des histoires » aux salariés, de cacher la réalité d'un voile de fictions trompeuses, mais aussi de faire partager un ensemble de croyances à même de susciter l'adhésion et d'orienter les flux d'émotions, bref de créer un mythe collectif contraignant. » (Salmon, 2007 p. 102)

<sup>353</sup> « There is a growing body of literature that focuses on the difficulties of work in multi- and interdisciplinary teams, citing issues of epistemological difference, conflicts of identity, group membership and cultural capital, misaligning of concepts and terminology, lack of openness to approaches and ideas from other disciplines, power issues, structural biases

enquête dépassent l'interrogation classique du rôle du sociologue dans la cité (Chenu, 1998 ; Callon, 1999 ; Trépos, 2001 ; Castel, 2002 ; Lahire, 2002 ; Becker, 2006 ; Piriou, 2006 ; Alter, 2008 ; Piriou, 2008). En effet, le déplacement de l'usage d'une pratique poétique à une pratique sibylline s'opère parallèlement à la diffusion de la légitimité de la critique (Callon, Lascoumes & Barthe, 2001). Puisque la projection se fait *au service de la recherche technologique*, elle s'inscrit dans une démarche de promotion de l'innovation. L'on peut ainsi envisager cette activité de promotion d'un point de vue idéaliste en l'associant à la créolisation comme « *un métissage d'arts, ou de langages qui produit de l'inattendu. C'est une façon de se transformer de façon continue sans se perdre. La créolisation s'applique non seulement aux organismes, mais aux cultures. Et les cultures sont des corps beaucoup plus complexes qu'un organisme. Si vous voulez, on peut prédire plus ou moins les résultats d'un métissage, mais non ceux de la créolisation. Prenez les langues créoles caraïbes, ou d'autres pays, ces résultats relèvent strictement du domaine de l'inattendu, de l'invention à foison de mots nouveaux, d'expressions, de blagues... Quand je dis que le monde se créolise, toute création culturelle ne devient pas créole pour autant, mais elle devient surprenante, compliquée et inextricablement mêlée aux autres cultures. La créolisation du monde, c'est la création d'une culture ouverte et inextricable, et elle se fait dans tous les domaines, musiques, arts plastiques, littérature, cinéma, cuisine, à une allure vertigineuse... La créolisation est une promotion de l'innovation.* » (Glissant, 1997 p. 38)

Cette vision d'une ronde des êtres, des savoirs et des compétences n'est pas si éloignée des observations que nous avons pu effectuer. Elle a au moins le mérite de renseigner sur la foi que nous entretenons dans la possibilité de faire émerger d'échanges improbables des matériaux robustes, actionnables et vraisemblables. Elle permet également de reconnaître que l'échec (la légende veut que 9 innovations sur 10 soient des échecs commerciaux) soit une variante intrinsèque de l'activité d'innovation. Elle permet d'envisager que le management de l'innovation, notamment lorsqu'il associe les sciences sociales comme partie prenantes, puisse favoriser le foisonnement de *compositions de fictions axiomatiques* comme des ressources précieuses à la conquête d'un monde de l'« après-Bachelard ». Enfin, à l'instar des carrières de l'usage que nous avons identifiées, elle nous offre la possibilité d'avoir confiance dans les bienfaits de la cohabitation d'exercices variés et pluriels de la science ou, au moins, de ce qui s'en réclame comme tel, sans plonger dans la tentation relativiste.

---

and failure of management. However this type of teams is constituted because it is recognised that their varying skills and knowledge are necessary to conduct research for innovation, in the same way as labour and knowledge is divided in most other areas of human endeavour. » (Stewart & Claeys, 2009)

## XIV - Conclusion de la partie IV

---

Dire le caractère *pro-politique* de la projection d'usage, c'est défendre la thèse que celle-ci se situe en un endroit autre que les objets traditionnels d'investigation des sciences ou des technologies « *telles qu'elles se font* ». Bien entendu, on peut d'abord recenser les similarités entre les résultats de notre investigation et les conclusions des STS. On y lit sans mal une conformité aux traits saillants mis en lumière par les sociologues des sciences et des techniques<sup>354</sup>. En ce sens, l'étude confirme ce que l'on sait déjà. L'étude ajoute cependant à ce socle de connaissances bien établi en apportant des précisions à ce qu'il se passe dans ces zones de conception technologique marquées du fer de l'incertitude (le FFE), de la coopération entre disciplines et de l'implication des sciences sociales comme technologie de conception.

Ainsi, le processus de projection d'usage est autant exposé aux contingences inhérentes à l'activité de conception que le sont les concepteurs traditionnellement étudiés. On l'a vu, la construction de la projection génère des déplacements, des arrangements<sup>355</sup> entre « *choses* », êtres, objets et types de médiations. On a pu voir également que la scénarisation n'a d'inébranlable que *l'enthousiasme technologique* sur lequel elle s'appuie. Le reste, c'est-à-dire ce sur quoi l'infrastructure se construit, est en co-construction : les « *choses* » ne sont pas stabilisées avant d'être versées à l'infrastructure, elles se fondent dans l'infrastructure simultanément à leurs processus de définition. Ainsi, le constat d'une *ultralocalité* et d'une *ultraperformativité* de la projection d'usage ne tient pas de l'inflation lexicale mais vise bien à souligner le fait que les lieux ne préexistent pas aux espaces, que les choses ne précèdent pas l'infrastructure. Chacun des termes, les lieux, surgit dans la pratique de l'espace infrastructurel.

Par ailleurs, et non sans lien, si l'infrastructure constitue bien une forme de stabilisation, elle n'en est pas pour autant le lieu de cristallisation des énoncés scientifiques. La projection d'usage n'est pas le lieu où se dessine la ligne de front qui distingue les

---

<sup>354</sup> On se réfère ici au travail de Michel Dubois (Dubois, 2001), pour qui, les STS sont structurées autour de trois propositions. Le fait que « la pratique scientifique repose sur une logique de l'« opportunisme », qu'elle soit « idiosyncratique » et que « les faits soient engendrés par des détails « contingents » de la pratique. » (p.116). Dans le même ordre d'idée, on peut citer l'introduction de l'ouvrage princeps de la sociologie des techniques de (Bijker & Law, 1992). Les éditeurs de l'ouvrage identifient quatre facteurs qui unissent le champ : le changement technologique est contingent, les technologies naissent du conflit, de la différence ou de la résistance, ces différences peuvent ou non donner lieu à des conflits, les technologies font partie de stratégies de ceux qui les défendent, et enfin que les conséquences de ces stratégies doivent être traitées comme des phénomènes émergents.

<sup>355</sup> Les sociologues des sciences et des techniques ont (Knorr, 1979 ; Latour & Woolgar, 1979 ; Clarke, A. & Fujimura, 1992 ; Hard, 1994 ; Nutch, 1996), nous revenons sur l'idée de tinkering et de bricolage dans la conclusion de la thèse.

« *faits* » des « *artefacts* »<sup>356</sup>. L'extérieur au projet (l'à venir probable) et l'intérieur du projet (l'énoncé à construire, conquérir et constater) se confondent dans l'horizon de conquêtes et de batailles futures, ici la conception du CPM. En effet, le temps de la projection d'usage est le temps du *pré-texte* de la technoscience : la pratique de ce territoire n'est que suite d'épreuves, d'articulation dont la présence ne permet pas seulement le bon déroulement du projet, mais en constitue l'essence. Cette révélation du travail d'articulation, qui passe du statut d'étai assurant la bonne marche du projet à clé de voute de la scénarisation, participe de l'ancrage de la projection d'usage hors du « *contexte de découverte* », soit le contexte d'obtention ou de découverte du résultat scientifique, et hors du « *contexte de justification* », soit les lieux où les résultats sont présentés et justifiés (Reichenbach, 1938)<sup>357</sup>. Ce qui est en voie de stabilisation durant le processus de projection d'usage, ce ne sont pas des énoncés mais plutôt des *axiomes* dont le renvoi étymologique évacue la question du « vrai » : un axiome est ce qui est considéré comme digne, convenable et évident en soi ; et qui a comme autre propriété d'être à la base de constructions scientifiques.

En se penchant de près sur la fabrique de cet *axiome* qu'est le scénario, nous avons mis à jour divers phénomènes de médiations, de traductions et de représentations donnant lieu à des convergences de choses – personnes, objets et lieux, qui elles-mêmes font place à des hybrides de choses<sup>358</sup>. L'ensemble de ces phénomènes nous amène à consolider le choix du vocable représentation au sens de présenter à nouveau, de représentation politique et de représentation publique (Latour, 2005) dans la dernière définition adoptée de la projection d'usage, soit la *représentation de fictions au service de la recherche technologique*. Nous choisissons d'enrichir cette définition par l'adjonction du caractère axiomatique de la

<sup>356</sup> « At the frontier of science, statements are constantly maintaining a double potential: they are either accounted for in terms of local causes (subjectivity or artefact) or are referred to as a thing “out there” (objectivity and fact) [...] The importance of observing the transformation of a statement between fact-like and artefact-like status is obvious: if the “truth effect” of science can be shown both to fold and unfold, it becomes much more difficult to argue that the difference between a fact and artefact is that the former is based on reality while the latter merely arises from local circumstances and psychological conditions. The distinction between reality and local circumstances *exists only after* the statement has stabilized as a fact. To summarize the argument in another way, “reality” cannot be used to explain why a statement becomes a fact, since it is only after it has become a fact that the effect of reality is obtained. This is the case whether the reality effect is cast in terms of “objectivity” or “out there-ness. It is *because* the controversy settles, that a statement splits into an entity and a statement about an entity; such a split never precedes the resolution of controversy. » (Latour & Woolgar, 1979)

<sup>357</sup> On pourrait même extrapoler et considérer les projections comme parentes du chat de Schrödinger en ce qu'elles échappent aux sens qui fondent les catégorisations habituelles.

<sup>358</sup> Notons que ces transformations touchent autant les « technologues » que les sociologues praticiens. En ce qui concerne ces derniers, le constat est identique dans des champs d'application différents : « Cherchant à faire émerger des projets ou des ajustements innovants, le sociologue praticien se situe entre l'institué et l'imaginaire. Il est du côté de l'institué puisqu'il ne peut pas faire fi de l'existant, mais il fait inévitablement appel à son imagination, cette dernière étant le moteur nécessaire à toute transformation. Imagination professionnelle et donc sociologique, il se doit aussi d'inciter les acteurs à mettre en éveil leur capacité imaginative afin de concevoir les solutions nouvelles les plus adaptées aux problèmes que les acteurs et lui-même cherchent à résoudre. De ce fait, si le praticien en sciences sociales agit sur l'objet d'intervention en participant à sa transformation et à l'émergence de projets créatifs, il joue nécessairement un rôle sur les acteurs de ces projets en conception. » (Legrand, 2004 p. 121)



projection en adoptant pour définition de la projection d'usage la *composition de fictions axiomatiques au service de la recherche technologique*.

## Conclusion générale

*“The future’s another country, man,’ said Carl mournfully,  
and then the punchline seemed to come to him;  
his face surrendered to a smile.  
‘And I still ain’t got a passport”  
(Smith, 2007 p. 140)*

Dans cette thèse, nous nous sommes concentrés sur l'un des modes d'existence de la projection d'usage, le scénario, pour interroger le rôle et la performance des recherches spéculatives pour l'innovation et de ceux qui participent à leur élaboration. Notre ambition était de rendre intelligibles les politiques mises en œuvre par ces recherches, la performance des collectifs mobilisés sur les recherches et sur eux-mêmes ainsi que les arrangements déployés par les acteurs durant ces processus. En définissant les projections d'usages comme des *compositions de fictions axiomatiques au service de la recherche technologique* nous nous sommes bornés à l'appréhension de celles-ci comme des *technologies de production de connaissances* qu'il nous a fallu disséquer en recourant à une large palette d'outils méthodologiques et conceptuels. Notre « composite » a nécessité la mobilisation de techniques d'observation participante, le recours aux enseignements de la sociologie interactionniste, l'utilisation d'outils issus de la linguistique et de la sémiologie afin de lire le produit de la projection, le parallélisme cher à la sociologie des sciences et des techniques pour lire la trajectoire des objets et des personnes dans la composition d'axiomes. Il nous a semblé nécessaire d'avoir recours à ce patchwork conceptuel pour répondre à notre problématique initiale :

*Comment les recherches spéculatives pour l'innovation, technologies particulières de réduction de l'incertitude planant sur le développement de l'innovation technologique, s'inscrivent concrètement dans les étapes amont des processus de conception ?*

Entamer notre travail par une analyse dynamique du concept d'usage, nous a permis de mettre en lumière l'impact des processus qui modifient les manières de penser et de faire la recherche au XXIème siècle. La description des trois carrières de l'usage et des mutations des pratiques associées (poétique, pythique et sibylline) est le reflet de mutations conjointes qui affectent la recherche académique comme la recherche industrielle : l'internationalisation des standards et des normes de recherche, la montée de régimes d'expertises de plus en plus pointues, la fertilisation croisée de disciplines et spécialités autrefois étanches, le montée en puissance des technologies de l'information et de la communication comme objet et outil de recherche, la remise en question de la légitimité des institutions de production de connaissance et la prolifération des lieux de contestation de ces discours légitimes. En somme, la convergence des SHS et des stratégies industrielles de la recherche et développement en micro et nanotechnologies est une donnée, un discours et un processus complexe de la modernité avancée. En analysant les carrières de l'usage, nous avons pu constaté qu'elle recouvrait une réalité due à la promotion et au travail d'acteurs intéressés, acteurs eux-mêmes parties prenantes de champs en pleine recomposition. La

projection d'usage en est un stigmat, une preuve ou une forme de divination, c'est selon, de cette convergence marquée par un régime de production scientifique transversal et structuré en projet.

En nous concentrons sur un type de projet spécifique, les projets de recherche et développement de micro et nanotechnologies du CEA Minatex, et en particulier sur les recherches spéculatives pour l'innovation, nous avons démontré la possibilité de stabiliser le processus de recherche malgré les contingences du « Fuzzy Front End » de l'innovation. La projection d'usage est d'abord l'élaboration d'écologies socio-techniques de l'usage. Elle participe d'une variété d'outils qui permettent, lors de leur élaboration, d'adjoindre à la définition d'un cadre de fonctionnement celle d'un cadre d'usage projeté, ce, afin de consolider une écologie socio-technique stable. Formellement, la scénarisation est une modalité de projection suffisamment souple pour intégrer des questionnements familiers des SHS.

Cependant, la projection d'usage, une fois stabilisée, ne constitue pas naturellement une « *perspective*<sup>359</sup> » (Borup, Brown, Konrad & Lente, 2006). Pour servir de point d'appui à la conception dont elles structurent l'activité, être pourvoyeuses de légitimité, provoquer l'intérêt, en somme pour se constituer comme « *point de passage obligatoire* » de l'entreprise de conception (Callon, 1986), les projections d'usage s'équipent de la puissance et de la force d'attraction de la fiction. Le scénario est un acte doublement performatif : au niveau du langage et au niveau de la croyance, il est une forme de démonstration de son efficacité et de son utilité propres. C'est bien à l'aune de sa transférabilité et de son interopérabilité que s'établit la mesure du retour sur investissement de la projection d'usage. Or, dans l'absence et l'impossibilité de mise à l'épreuve réelle de celle-ci, la recherche d'un degré de vraisemblance satisfaisant des projections sert d'arrangement et de lien entre le présent et le futur, le mondain et le scientifique. La marque de l'enthousiasme technologique sur les ordonnancements de collectifs créés par la fiction est aussi puissante qu'est vaine la volonté affichée de promouvoir une démocratie dialogique dans la conception des technologies. Pour assurer la bonne marche du projet, et toujours dans l'optique de stabiliser autant que faire se peut les éléments fuyants du projet, l'usage est projeté le jeu de la représentation d'intérêts d'entités en devenir. La légitimité des mandants est cependant peu discutée, dans le cadre du projet, au profit du bon fonctionnement de celui-ci.

Directement liée à cet impératif de maximisation du profit au regard des ressources allouées, autrement dit de la priorité du retour sur investissement, la projection d'usage, en tant que processus, entraîne de forte recomposition de la nature des choses qui y sont

---

<sup>359</sup> Notre traduction. Le terme original est « *expectation* ».

engagées afin de se composer elle-même comme infrastructure frontière ultralocale et ultraperformative. Ultralocale, car chaque lieu qui la compose émerge de la pratique de la projection. Ultraperformative, car le lieu de la projection ne préexiste pas à l'espace de sa pratique : ils se créent concomitamment. Sur le plan politique de distribution classique des prérogatives, caractéristique de l'expertise stratifiée, la projection d'usage bouscule les rôles définis en faisant émerger des genres (de choses et de personnes) hybrides : les borderlands. Cette déportation du travail de recherche hors du débat scientifique, sur le terrain axiomatique, est aussi celle qui autorise la projection à sortir des conditions locales de sa production en la dotant de caractéristiques peu discutables, une fois celle-ci stabilisée.

Nous l'avons donc vu, la projection d'usage est une forme de réponse à une demande sociale qui émane de plusieurs endroits et dont l'exigence de production de savoirs actionnables nécessite de composer avec des données en mouvement. Les sciences sociales y jouent les rôles d'expert à la fois mandaté, traitant et instituant au risque d'une perte de légitimité interne et externe et au profit d'une inventivité certaine. Cependant, si l'espace de la critique propre à leur formation peut être réduit durant l'établissement des diagnostics et devant la force des principes de véridiction et d'inférence, on peut nourrir l'espoir que la diffusion de leur propre réflexivité ne puisse être que stimulante et enrichissante. Stimulante, d'abord, dans les lieux de leur propre pratique, comme véhicule d'une remise en question des cadres de pensées déterministes majoritaire dans le monde des techno-sciences. Enrichissante, enfin, dans les agoras émergentes de constitution du débat sur les sciences, qu'il s'agisse de lieux de la recherche académique ou de ceux au sein desquels le débat public prend place.

# Bibliographie

- (16 décembre 2008). « Décision n°1350/2008/CE du Parlement européen et du Conseil concernant l'Année européenne de la créativité et de l'innovation (2009) ».
- (2008) *Annexe Technique au projet COPRIM*.
- Abric J.-C. (éd.) (1994) *Pratiques sociales et représentations* coll. Psychologie sociale. Paris, Presses universitaires de France.
- Agnieszka Z. (2005). « Evaluating Wireless Technologies in Mobile Payments: A Customer Centric Approach ». *Proceedings of the International Conference on Mobile Business*, IEEE Computer Society.
- Agre P.E. (1994). « From high tech to human tech: Empowerment, measurement, and social studies of computing », *Computer Supported Cooperative Work (CSCW)*, vol. 3, no° 2, p. 167-195.
- Agre P.E. et Rotenberg M. (éd.) (1998) *Technology and Privacy: The New Landscape*, The MIT Press.
- Akrich M. (1989 ). « La construction d'un système socio-technique. Esquisse pour une anthropologie des techniques », *Anthropologie et sociétés*, vol. 13, no° 2, p. 31-54.
- Akrich M. (1992). « The De-Description of Technical Objects », in Bijker, W. et Law, J. (éd.) (1992). *Shaping Technology/Building Society*, Cambridge, London, The MIT Press, p. 205-224.
- Akrich M. (1993). « Les objets techniques et leurs utilisateurs. De la conception à l'action », *Raisons pratiques*, vol. 4, p. 35-57.
- Akrich M. (1995). « User Representations : Practices, Methods and Sociology », in Rip, A., Misa, T.J. et Schot, J. (éd.) (1995). *Managing technology in society. The approach of constructive technology assessment*, London, Pinter, p. 167-184.
- Akrich M. (2001). « De l'accusation à la cause : L'intégration des controverses et des conflits dans le processus d'innovation », in Goujon, P. et Hériard Dubreuil, B. (éd.) (2001). *Technology and Ethics. A European Quest for Responsible Engineering*, Leuven, Peeters, p. 157-167.
- Akrich M., Callon M. et Latour B. (1991). « A quoi tient le succès des innovations? L'art de choisir les bons porte-parole », in Vinck, D. (éd.) (1991). *Gestion de la recherche*, Bruxelles, De Boeck, p. 53-76.
- Akrich M., Callon M. et Latour B. (1991). « A quoi tient le succès des innovations? L'art de l'intéressement », in Vinck, D. (éd.) (1991). *Gestion de la Recherche. Nouveaux problèmes, nouveaux outils*, Bruxelles, De Boeck, p. 27-52.
- Akrich M., Callon M. et Latour B. (éd.) (2006) *Sociologie de la traduction : Textes fondateurs*. Paris, Presses de l'Ecole des Mines.
- Akrich M. et Latour B. (1992). « A Summary of a Convenient Vocabulary for the Semiotics of Human and Nonhuman Assemblies », in Bijker, W. et Law, J. (éd.) (1992). *Shaping Technology/Building Society*, Cambridge, London, The MIT Press, p. 259-264.
- Alter N. (1999). « La sociologie et les métiers de l'analyse », *Sociologie pratique*, no° 2, p. 99-108.
- Andersen E.S. et Lundvall B.A. (1988). « Small National Systems of Innovation Facing Technological Revolutions : An Analytic Framework », in Freeman, C. et Lundvall, B.A. (éd.) (1988). *Small Countries Facing the Technological Revolution*, London and New York, Pinter Publishers, p. 9-36.
- Anjembe E., Michalon J. et Emprun C. (17 novembre 2009). « Faire science sur les sciences: postures et expériences doctorales », in Journées annuelles du cluster 14 de la région Rhône-Alpes, E.e.r.d.l.s., de la technique et de leurs usages (éd.), Lyon.
- Antoniou Z. et Varadan S. (2007). « Proceedings of the Third international Conference on Wireless and Mobile Communications », (*ICWMC'07*), IEEE Computer Society.
- Ariès P. et Duby G. (éd.) (1999) *Histoire de la vie privée*. Paris, Points.



- Arnall T. (2006). « A graphic language for touch-based interactions », *Proceedings of Mobile Interaction with the REal World*.
- Augé M. (1992). *Non-lieux : introduction à une anthropologie de la surmodernité*, Paris, Seuil.
- Augustin S. (1998). *Confessions, Livre XI*, Paris, Nathan.
- Auvray F. (1975). *Comment rentabiliser la recherche et le développement, choix, conduite et optimisation des projets*, Paris, Entreprise moderne d'édition.
- Axtell C.M., Waterson P.E. et Clegg C.W. (1997). « Problems integrating user participation into software development », *Int. J. Hum.-Comput. Stud.*, vol. 47, no° 2, p. 323-345.
- Backman F. et Rozenberg O. (2009). « Mortels transferts? La pratique des entretiens collectifs par les Grands Instituts de Sondages Internationaux et par la recherche en Science Sociale », in Focus groupes, e.c.é.d.l.-J.d.é.d.g.M.d.l.A. (éd.), Paris.
- Bannon et Liam (1992). « From human factors to human actors: the role of psychology and human-computer interaction studies in system design » (1992). *Design at work*, L. Erlbaum Associates Inc., p. 25-44.
- Bardini T. et Horvath A. (1995). « The social construction of the personal computer user », *Journal of Communication*, vol. 45, no° 3, p. 40-66.
- Battarbee K. (2003). « Defining co-experience ». *Proceedings of the 2003 international conference on Designing pleasurable products and interfaces*, Pittsburgh, PA, USA, ACM.
- Beck U. (1986). *Risikogesellschaft: Auf dem Weg in eine andere Moderne*, Francfort, Suhrkamp Verlag.
- Becker H.S. (2006 ). *Le travail sociologique. Méthode et substance*, Fribourg, Academic Press.
- Bell D. (2006). *Science, Technology and Culture*, Open University Press.
- Bell G., Blythe M., Gaver B., et al. (2003). « Designing culturally situated technologies for the home ». *CHI '03 extended abstracts on Human factors in computing systems*, Ft. Lauderdale, Florida, USA, ACM.
- Bellotti V. (2001). « Design for Privacy in Multimedia Computing and Communications Environments », in Agre, P.E. et Rotenberg, M. (éd.) (2001). *Technology and Privacy: The New Landscape*, Cambridge, The MIT Press, p. 63-98.
- Bellotti V. et Sellen A. (1993). « Design for privacy in ubiquitous computing environments », *ECSCW'93: Proceedings of the third conference on European Conference on Computer-Supported Cooperative Work*, Kluwer Academic Publishers.
- Benyo B., Vilmos A., Kovacs K. et Kutor L. (2007). « NFC Applications and Business Model of the Ecosystem », *Mobile and Wireless Communications Summit, 16th IST*, IEEE
- Berg M. (1998). « The Politics of Technology: On Bringing Social Theory into Technological Design », *Science, Technology & Human Values*, vol. 23, no° 4, p. 456-490.
- Bessy C. et Chateauraynaud F. (1995). *Experts et faussaires. Pour une sociologie de la perception*, Paris, Métailié.
- Bijker W. (1992). « The Social Construction of Fluorescent Lighting, or How an Artifact Was invented in Its Diffusion Stage », in Bijker, W. et Law, J. (éd.) (1992). *Shaping Technology/Building Society*, Cambridge, London, The MIT Press, p. 75-102.
- Bijker W. (1993). « Do Not Despair: There Is Life After Constructivism », *Science, Technology & Human Values*, vol. 18, no° 1, p. 113-138.
- Bijker W. et Law J. (1992). « General Introduction », in Bijker, W. et Law, J. (éd.) (1992). *Shaping Technology/Building Society*, Cambridge, London, The MIT Press, p. 1-14.
- Bijker W. et Law J. (éd.) (1992) *Shaping Technology/Building Society*. Cambridge, London, The MIT Press.

- Bijker W.E. (1987). « The social construction of bakelite : toward a theory of invention », in Bijker, W.E., Hugues, T.P. et Pinch, T. (éd.) (1987). *The social construction of technological systems. New directions in the sociology and history of technology.*, Cambridge, London, The MIT Press, p. 159-190.
- Bijker W.E., Hugues T.P. et Pinch T. (éd.) (1989) *The Social Construction of Technological Systems. New directions in the Sociology and History of Technology.* Cambridge, London, The MIT Press.
- Bjerknes G. et Bratteteig T. (1995). « User participation and democracy: a discussion of Scandinavian research on systems development », *Scand. J. Inf. Syst.*, vol. 7, no° 1, p. 73-98.
- Blomberg J., Suchman L. et Trigg R., H. (1996). « Reflections on a Work-Oriented Design Project », *Hum.-Comput. Interact.*, vol. 11, p. 237-265.
- Bloomberg J. (1993). « Ethnographic field methods and their relation to design », in Schuler, D. et Namioka, A. (éd.) (1993). *Participatory Design. Principles and Practices*, Hillsdale, NJ, Lawrence Erlbaum Associate, p. 79-97.
- Blythe M., Overbeeke K., Monk A.F. et Wright P.C. (2003). *Funology: from usability to enjoyment*, Dordrecht, Kluwer.
- Blythe M., Wright P., McCarthy J. et W. Bertelsen O. (2006). « Theory and method for experience centered design ». *CHI '06 extended abstracts on Human factors in computing systems*, Montréal, Québec, Canada, ACM.
- Bodker S. (1996). « Creating Conditions for Participation: Conflicts and Resources in Systems Development », *Hum.-Comput. Interact.*, vol. 11, p. 215-236.
- Bodker S. (1998). « Understanding representation in design », *Hum.-Comput. Interact.*, vol. 13, no° 2, p. 107-125.
- Bodker S. (1999). « Scenarios in User-Centered Design - Setting the Stage for Reflection and Action ». *Proceedings of the Thirty-Second Annual Hawaii International Conference on System Sciences-Volume 3 - Volume 3*, IEEE Computer Society.
- Bodker S. et Christiansen E. (1997). « Scenarios as Springboards in CSCW Design », in Bowker, G., Star, S.L., Turner, W. et Gasser, L. (éd.) (1997). *Social Science, Technical Systems, and Cooperative Work: Beyond the Great Divide*, Lawrence Erlbaum Associates, p. 217-234.
- Borup M., Brown N., Konrad K. et Lente H.v. (2006). « The Sociology of Expectations in Science and Technology », *Technology Analysis and Strategic Management*, vol. 18, no° 3/4, p. 285-298.
- Boujut J.-F. et Blanco E. (2003). « Intermediary Objects as a Means to Foster Co-operation in Engineering Design », *Comput. Supported Coop. Work*, vol. 12, no° 2, p. 205-219.
- Boullier D. (1994). « Construire le téléspectateur: récepteur, consommateur ou citoyen », in Vitalis, A. (éd.) (1994). *Médias et nouvelles technologies. Pour une socio-politique des usages*, Rennes, Apogée.
- Boullier D. (1997). « La connaissance stratégique des usages », *Conseil scientifique de France Télécom*.
- Bourdieu P. (1980). *Le sens pratique*, Paris, Minuit.
- Bourdieu P., Chamboredon J.-C. et Passeron J.C. (1983). *Le métier de sociologue*, Paris, EHESS.
- Boutinet J.-P. (2007). *Anthropologie du projet*, Paris, PUF.
- Bowers J. et Martin D. (2003). « Making the Organisation Come Alive: Talking Through and About the Technology in Remote Banking », *Hum.-Comput. Interact.*, vol. 18, no° 1-2, p. 111-148.
- Bowker G. et Star S.L. (1999). *Sorting Things Out : Classification and Its Consequences*, Boston, MIT Press.

- Bretagne V. (2004). « Employeurs de sociologues: compétences expertes et réflexivité », in Legrand, M. et Vrancken, D. (éd.) (2004). *L'expertise du sociologue* Paris, L'Harmattan, p. 143-180.
- Bruce J. (1987). « Users' perspectives on contraceptive technology and delivery systems highlighting some feminist issues », *Technology in Society*, vol. 9, no° 3-4, p. 339-358.
- Brugidou M. (2008). *L'opinion et ses publics. Une approche pragmatiste de l'opinion publique*, Paris, Presses de la Fondation nationale des sciences politiques.
- Bucciarelli L. (1994). *Designing engineers*, Cambridge, MA, MIT Press.
- Button G. (2000). « The ethnographic tradition and design », *Design Studies*, vol. 21, no° 4, p. 319-332.
- Button G. et Dourish P. (1996). « Technomethodology: paradoxes and possibilities », *Proceedings of the SIGCHI conference on Human factors in computing systems: common ground*, Vancouver, British Columbia, Canada, ACM.
- Callon M. (1986). « Some Elements of a Sociology of Translation : Domestication of the Scallops and the Fisherman of St. Brieux Bay », in Law, J. (éd.) (1986). *Power, Action and Belief : a New Sociology of Knowledge?*, London, Routledge and Kegan, p. 196-233.
- Callon M. (1999). « Ni intellectuel engagé, ni intellectuel dégaillé : la double stratégie de l'attachement et du détachement », *Sociologie du travail*, no° 41, p. 65-78.
- Callon M. et Law J. (1989). « On the Construction of Sociotechnical Networks: Content and Context Revisited », *Knowledge and Society*, vol. 9, p. 57-83.
- Camus A. (1942). *Le mythe de Sisyphe*, Paris, Gallimard.
- Cardon D. (1997). « Les sciences sociales et les machines à coopérer. Une approche bibliographique du Computer Supported Cooperative Work (CSCW) », *Réseaux*, vol. 15, no° 85, p. 13-51.
- Carlile P.R. (2002). « A Pragmatic View of Knowledge and Boundaries: Boundary Objects in New Product Development », *Organization Science*, vol. 13, no° 4, p. 442-455.
- Carlson B.W. (1992). « Artifacts and Frames of Meaning: Thomas A. Edison, His Managers, and the Cultural Construction of Motion Pictures », in Bijker, W. et Law, J. (éd.) (1992). *Shaping Technology/Building Society*, Cambridge, London, The MIT Press, p. 175-198.
- Carroll J.M. (1999). « Five Reasons for Scenario-Based Design », *Proceedings of the 32nd Hawaii International Conference on System Sciences*, Hawaii.
- Carroll J., M. (1996). « Encountering others: reciprocal openings in participatory design and user-centered design », *Hum.-Comput. Interact.*, vol. 11, no° 3, p. 285-290.
- Carroll J., Rosson M.B. et McInerney P. (2003). « Scenarios in practice », *CHI '03 extended abstracts on Human factors in computing systems*, Ft. Lauderdale, Florida, USA, ACM.
- Cefaï D. (2002). « Qu'est-ce qu'une arène publique? Quelques pistes pour une approche pragmatiste », in Cefaï, D. et Isaac, J. (éd.) (2002). *L'Héritage du pragmatisme. Conflits d'urbanité et épreuves de civisme*, La Tour d'Aigues, Editions de l'Aube.
- Chalas Y., Gilbert C. et Vinck D. (éd.) (2009) *Comment les acteurs s'arrangent avec l'incertitude*. Paris, Editions des archives contemporaines.
- Chambat P. (1994). « NTIC et représentation des usagers », in Vitalis, A. (éd.) (1994). *Médias et nouvelles technologies. Pour une socio-politique des usages*, Rennes, Apogée, p. 45-59.
- Chambat P. (1994). « NTIC et représentations des usages », in Vitalis, A. (éd.) (1994). *Médias et nouvelles technologies. Pour une socio-politique des usages*, Rennes, Editions Apogée, p. 45-59.

- Chavira G., Nava S., Hervas R., *et al.* (2007). « Combining RFID and NFC Technologies in an Aml Conference Scenario ». *Proceedings of the Eighth Mexican International Conference on Current Trends in Computer Science*, IEEE Computer Society.
- Clarke A. (2005). *Situational analysis: grounded theory after the postmodern turn*, Thousands Oaks, Sage.
- Clarke A. et Fujimura J. (éd.) (1992) *The right tools for the job: At work in the twentieth century life sciences*. Princeton, NJ, Princeton University Press.
- Clarke A. et Montini T. (1993). « The Many Faces of RU486: Tales of Situated Knowledges and Technological Contestations », *Science, Technology, & Human Values*, vol. 18, no° 1, p. 42-78.
- Clausen H. (1993). « Narratives as tools for the system designer », *Design Studies*, vol. 4, no° 3, p. 283-298.
- Clement A. (1994). « Considering Privacy in the Development of Multimedia Communications », *Computer-Supported Cooperative Work*, vol. 2, p. 67-88.
- Clemmensen T. (2004). « Four approaches to user modelling—a qualitative research interview study of HCI professionals' practice », *Interacting with computers*, vol. 16, no° 4, p. 799-829.
- Cockburn A. (2001). *Rédiger des cas d'utilisation efficaces*, Paris, Eyrolles.
- Collins H.M. et Evans R. (2007). *Rethinking expertise*, University of Chicago Press.
- Collins H.M. et Pinch T. (1982). *Frames of Meaning : The Social Construction of Extraordinary Science*, Boston, Routledge and Kegan Paul.
- Cooper A. (1999). *The Inmates Are Running the Asylum*, Indianapolis, SAMS.
- Cooper R.G. et Kleinschmidt E.J. (1993). « Screening new products for potential winners », *Long Range Planning*, vol. 26, no° 6, p. 74-81.
- Cornu G. (1987). *Vocabulaire juridique*, Paris, Quadrige/ PUF.
- Crippa S. (1999). « Entre vocalité et écriture: les voix de la Sibylle et les rites vocaux des magiciens », in Batsch, C., Egelhaaf-Gaiser, U. et Stepper, R. (éd.) (1999). *Zwischen Krise und Alltag. Conflit et normalité*, Stuttgart, Steiner, p. 95-110.
- Csaposi M. et Nagy A. (2007). « New Applications for NFC Devices », *Mobile and Wireless Communications Summit, 16th IST*, IEEE.
- D'Avenir R.A. et Gunther R.E. (1994). *Hypercompetition: managing the dynamics of strategic maneuvering*, New York, Free Press.
- David P.A. (1986). « Understanding the Economics of QWERTY », in Parker, W.N. (éd.) (1986). *Economic History and the Modern Economist*, Oxford, Basil Blackwell.
- De Certeau M. (1990). *L'invention au quotidien*, Paris, Gallimard.
- De Gournay C. (1997). « Du téléphone et du congélateur : le communiquer frais », in Obadia, A. (éd.) (1997). *Entreprendre la ville [Actes du Colloque de Cerisy]*, La Tour d'Aigues, Editions de l'Aube, p. 229-267.
- Deleuze G. et Guattari f. (1980). *Mille Plateaux*, Paris, Editions de Minuit.
- Despret V. (2002). *Quand le loup habitera avec l'agneau*, Paris, Les empêcheurs de penser en rond.
- Dewey J. (1927). *The Public and its Problems*, New York, Henry Holt & Co.
- DiSalvo C. (2009). « Design and the Construction of Publics », *Design Issues*, vol. 25, no° 1, p. 48-63.
- Dix A., Finlay J., Abowd G. et Beale R. (1993). *Human-Computer Interaction*, Hemel Hempstead, Prentice Hall.
- Dourish P. (2001). *Where the action is*, Cambridge, MA, MIT Press.
- Dourish P., Grinter R., Delgado et Joseph M. (2004). « Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem », *Personal and Ubiquitous Computing*, vol. 8, no° 6, p. 391-401.

- Dubey G. et Moricot C. (2006) *La polyvalence du rafale ou l'objet total. La relation entre une technologie nouvelle et ses utilisateurs*. (C2SD, L.d.d.). Paris, Ministère de la défense.
- Dubois M. (2001). « Le relativisme cognitif comme "moulin à vent"? », in Kremer-Marietti, A. (éd.) (2001). *Ethique et épistémologie autour du livre "impostures intellectuelles" de Sokal et Bricmont*, Paris, L'Harmattan, p. 109-135.
- Durand G. (1988). « Le(s) grand(s) changement(s) ou l'après Bachelard », *Les Cahiers de l'imaginaire*, no° 1, p. 5-15.
- Ehn P. (1988). *Work-oriented Design of Computer Artifacts*, Falköping, Arbetslivcentrum.
- Epstein S. (2003). « Inclusion, Divesity, and Biomedicl Knowledge Making : The Multiple Politics of Representation », in Oudshoorn, N. et Pinch, T. (éd.) (2003). *How users matter. The co-construction of users and technologies*, Cambridge, London, The MIT Press, p. 173-190.
- Erickson T. (1995). « Notes on Design Practice: Stories and Prototypes as Catalysts for Communication », in Carroll, J.M. (éd.) (1995). *Scenario-Based Design. Envisioning Work and Technology in System Development*, Wiley & Sons.
- Etkowitz H. (1998). « The Norms of Entrepreneurial Science: Cognitive Effects and the New University-Industry Linkages », *Research Policy*, vol. 27, no° 8, p. 823-833.
- Etzioni A. (1999). *The Limits of Privacy*, New York, Basic Books.
- Falke O., Ruzkio E., Dietz U., et al. (2007) *Mobile Service for Near Field Communication*. Munich, University of Munich. Department of Computer Science. Media Informatics Group.
- Fallman D. (2008). « The Interaction Design Research Triangle of Design Practice, Design Studies, and Design Exploration », *Design Issues*, vol. 24, no° 3, p. 4-18.
- Feenberg A. (2004). *(Re)penser la technique. Vers une technologie démocratique*, Paris, La Découverte.
- Fleck J. (1994). « Learning by trying: the implementation of configurational technology », *Research Policy*, vol. 23, no° 6, p. 637-652.
- Flichy P. (2003). *L'innovation technique. Récents développements en sciences sociales*, Paris, La Découverte.
- Flichy P. (2008). « Technique, usage et représentations », *Réseaux*, vol. 2, no° 148-149, p. 147-174.
- Floyd C. (1987). « Outline of a paradigm change in software engineering », in Bjerknes, G., Ehn, P. et Kyng, M. (éd.) (1987). *Computers and Democracy - a Scandinavian Challenge*, Avebury, Aldershot, p. 191-212.
- Forlizzi J. et Ford S. (2000). « The building blocks of experience: an early framework for interaction designers », *Proceedings of the 3rd conference on Designing interactive systems: processes, practices, methods, and techniques*, New York City, New York, United States, ACM.
- Forum N. (2008). "Frequently asked questions." Retrieved 21/02, 2008, url: <http://www.nfc-forum.org/resources/>.
- Fujimura J. (1992). « Crafting Science: Standardized Packages, Boundary Objects, and 'Translation' », in Pickering, A. (éd.) (1992). *Science as Practice and Culture*, Chicago, University of Chicago Press, p. 168-211.
- Fuller S. (1988). *Social epistemology*, Bloomington, Indiana University Press.
- Galison P. (1997). *Image and logic: A material culture of microphysics*, Chicago, The University of Chicago Press.
- Gaver B. et Martin H. (2000). « Alternatives: exploring information appliances through conceptual design proposals », *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, The Hague, ACM.
- Gentès A. (2008). « Design et médiation créative dans les technologies de l'information », *Hermès*, no° 50, p. 83-89.

- Gerson E. et Star S.L. (1986). « Analyzing Due Process in the Workplace », *ACM Transactions on Office Information Systems*, no° 4, p. 257-270.
- Gerson E. et Star S.L. (1986). « Analyzing due process in the workplace », *ACM Trans. Inf. Syst.*, vol. 4, no° 3, p. 257-270.
- Giddens A. (1990). *The Consequences of Modernity*, Stanford, Stanford University Press.
- Giere R.N. (1993). « Science and technology studies: Prospects for an enlightened postmodern synthesis », *Science, Technology & Human Values*, vol. 18, no° 1, p. 102-112.
- Gieryn T.F. (1983). « Boundary-Work and the Demarcation of Science from Non-Science: Strains and Interests in Professional Ideologies of Scientists », *American Sociological Review*, vol. 48, no° 6, p. 781-795.
- Gillier T. (2010). *Comprendre la génération des objets de coopération interentreprises par une théorie des co-raisonnements de conception*. Thèse de doctorat en Génie des Systèmes Industriels, Institut National Polytechnique de Lorraine (Grenoble).
- Glissant E. (1997). *Traité du Tout-Monde*, Paris, Gallimard.
- Goffman E. (1973). *La Mise en scène de la vie quotidienne. 1. La Présentation de soi*, Paris, Minuit.
- Goffman E. (1991). *Les cadres de l'expérience*, Paris, Minuit.
- Gorman M.E., Groves J.F. et Catalano R.K. (2004). « Societal dimensions of nanotechnology », *IEEE Technology and Society Magazine*, vol. 29, no° 4, p. 55-64.
- Gould J.D. et Lewis C. (1985). « Designing for usability: Key principles and what designers think », *Communications of The ACM*, vol. 28, no° 3, p. 300-311.
- Gouldner A.W. (1970). *The Coming Crisis of Western Sociology*, New York, NY, Basic Books, Inc.
- Granjou C. (2004). *La gestion du risque: entre technique et politique. Comités d'experts et dispositifs de traçabilité à travers les exemples de la vache folle et des OGM*. Thèse de Doctorat en Sociologie, Université René Descartes (Paris V) (Paris).
- Grawitz M. (1996). *Méthodes des sciences sociales*, Paris, Dalloz.
- Green N., Harper R.H.R., Murtagh G. et Cooper G. (2001). « Configuring the Mobile User: Sociological and Industry Views », *Personal Ubiquitous Comput.*, vol. 5, no° 2, p. 146-156.
- Greenbaum J. et Kyng M. (éd.) (1991) *Design at Work: Cooperative Design of Computer Systems* Hillsdale, NJ, Lawrence Erlbaum.
- Griesemer J. et Star S. (1989). « Institutional Ecology, Translations and Boundary Objects: Amateurs and Professionals in Berkeley's Museum of Vertebrate Zoology (1907-1939) », *Social Studies of Sciences*, vol. 19, p. 387-420.
- Grudin J. (1993). « Obstacles to participatory design in large product development organisations », in Schuler, D. et Namioka, A. (éd.) (1993). *Participatory design. Principles and practices*, Hillsdale, NJ, Lawrence Erlbaum Associates, p. 99-119.
- Guillaume M. (1997). « Articulation entre les échanges immatériels : présentation », in Obadia, A. (éd.) (1997). *Entreprendre la ville [Actes du Colloque de Cerisy]*, La Tour d'Aigues, Editions de l'Aube, p. 229-267.
- Habermas J. et Quéré L. (1989). « Médias de communication et espaces publics », *Réseaux*, vol. 7, no° 34, p. 79-96.
- Habermeier K.F. (1990). « Product use and product improvement », *Research Policy*, vol. 19, no° 3, p. 271-283.
- Hamlett P.W. (2003). « Technology Theory and Deliberative Democracy », *Science, Technology & Human Values*, vol. 28, no° 1, p. 112-140.
- Haraway D. (1991). « A Cyborg Manifesto: Science, Technology, and Socialist-Feminism in the Late Twentieth Century », in Haraway, D. (éd.) (1991). *Simians, Cyborgs and Women: The Reinvention of Nature* New York, Routledge, p. 149-181.

- Hard M. (1993). « Beyond Harmony and Consensus: A Social Conflict Approach to Technology », *Science, Technology & Human Values*, vol. 18, no° 4, p. 408-432.
- Hard M. (1994). « Technology as practice: Local and global closure in diesel-engine design », *Social Studies of Science*, vol. 24, no° 3, p. 549-585.
- Harold P. (2005). « Close up and in the comfort zone, Near Field Communication gets the message across », *Philips Research Password*, p. 18-24.
- Haselsteiner E. et Breitfuss K. (2006). « Security in near field communication (NFC) », *Printed handout of Workshop on RFID Security RFIDSec*.
- Hassenzahl M. (2004). « The interplay of beauty, goodness, and usability in interactive products », *Hum.-Comput. Interact.*, vol. 19, no° 4, p. 319-349.
- Hawkins R.R.M. et Shea J. (éd.) (1995) *Standards, Innovation and Competitiveness: The Politics and Economics of Standards in Natural and Technical Environments*, Edward Elgar Publishing Company.
- Heath C. et Luff P. (1992). « Collaboration and Control: Crisis Management and Multimedia Technology in London Underground Line Control Rooms », *Comput. Supported Coop. Work*, vol. 1, no° 1, p. 24-48.
- Henderson K. (1991). « Flexible Sketches and Inflexible Data Bases: Visual Communication, Conscription Devices, and Boundary Objects in Design Engineering », *Science, Technology & Human Values*, vol. 16, no° 4, p. 448-473.
- Henderson K. (1998). « The Role of Material Objects in the Design Process: A Comparison of Two Design Cultures and How They Contend with Automation », *Science, Technology & Human Values*, vol. 23, no° 2, p. 138-174.
- Hennion A. (1989). « An Intermediary between Production and Consumption: The Producer of Popular Music », *Science, Technology, & Human Values*, vol. 14, no° 4, p. 400-424.
- Highsmith J. (2002). *Agile Software Development Exosystems: Problems, Practices, and Principles*, Addison-Wesley.
- Hirschheim R. et Klein H.K. (1989). « Four paradigms of information systems development », *Commun. ACM*, vol. 32, no° 10, p. 1199-1216.
- Hugues T.P. (1986). « The Seamless Web: Technology, Science, Etcetera, Etcetera », *Social Studies of Science*, vol. 16, no° 2, p. 281-292.
- Hutchins E. (1995). *Cognition in the wild*, Cambridge, Usa, MIT Press.
- Hymes D. (1968). « Pidginization and creolisation of languages, their social contexts », *Item*, vol. 22.
- Jacobson I. (1995). « The Use-Case Construct in Object Oriented Software Engineering », in Carroll, J.M. (éd.) (1995). *Scenario based design. Envisioning work and technology in system development*, New York, Wiley, p. 85-108.
- Jaffro L. et Labrune M. (éd.) (1996) *Gradus Philosophique*. Paris, Flammarion.
- Jaureguiberry F. (2008). « De l'usage des technologies de l'information et de la communication comme apprentissage créatif », *Education et Sociétés*, vol. 2, no° 22, p. 29-42.
- Jeantet A. (1998). « Les objets intermédiaires dans la conception », *Sociologie du travail*, vol. 40, no° 3/98, p. 291-316.
- Jodelet D. (éd.) (1997) *Les représentations sociales* coll. Sociologie d'aujourd'hui. Paris, Presses universitaires de France.
- Jones J.C. (1988). « Softecnic », in Thackara, J. (éd.) (1988). *Design after modernism: beyond the object*, London, Thames and Hudson, p. 216-226.
- Jouët J. (2000). « Retour critique sur la sociologie des usages », *Réseaux*, vol. 18, no° 100, p. 487-521.
- Joyce J. (1992). *Portrait de l'artiste en jeune homme*, Paris, Gallimard.
- Junker B.H. (1960). *Field Work*, Chicago, The University of Chicago Press.

- Karat J. (1997). « Evolving the scope of user-centered design », *Communications of The ACM*, vol. 40, no° 7, p. 33-38.
- Kaye J.J., Boehner K., Laaksolahti J. et Stahl A. (2007). « Evaluating experience-focused HCI ». *CHI '07 extended abstracts on Human factors in computing systems*, San Jose, CA, USA, ACM.
- Kensing F. et Blomberg J. (1998). « Participatory Design: Issues and Concerns », *Comput. Supported Coop. Work*, vol. 7, no° 3-4, p. 167-185.
- Khurana A. et Rosenthal S.R. (1998). « Towards Holistic "Front Ends" In New Product Development », *Journal of Product Innovation Management*, vol. 15, no° 1, p. 57-74.
- Kline R. et Pinch T. (1996). « Users as Agents of Technological Change: The Social Construction of the Automobile in the Rural United States », *Technology and Culture*, vol. 37, no° 4, p. 763-795.
- Knorr K.D. (1979). « Tinkering toward success: Prelude to a theory of scientific practice », *Theory and Society*, vol. 8, no° 3, p. 347-376.
- Koch L. et Stermerding D. (1994). « The sociology of entrenchment: A cystic fibrosis test for everyone? », *Social Science & Medicine*, vol. 39, no° 9, p. 1211-1220.
- Koen P.A., Ajamian G.M., Clamen A., et al. (2001). « Providing Clarity and a Common Language to the "Fuzzy Front End" », *Research Technology Management*, vol. 44, no° 2, p. 46-55.
- Kuhn T.S. (1970). *The structure of scientific revolutions*, Chicago, University of Chicago press.
- Kujala S. (2002). *User studies: a practical approach to user involvement for gathering user needs and requirements.*, Acta Polytechnica Scandinavica, Mathematics and Computing Series No. 116, the Finnish Academies of Technology (Espoo).
- Kyng M. (1995). « Creating Contexts for Design », in Carroll, J.M. (éd.) (1995). *Scenario-Based Design. Envisioning Work and Technology in System Development*, New York, Wiley, p. 85-108.
- Lahire B. (2002). « Utilité : entre sociologie expérimentale et sociologie sociale », in Lahire, B. (éd.) (2002). *A quoi sert la sociologie*, Paris, La Découverte, p. 43-66.
- Langheinrich M. (2001). « Privacy by Design -- Principles of Privacy-Aware Ubiquitous Systems », *Proceedings of the Third International Conference on Ubiquitous Computing (UbiComp 2001)*, Atlanta, Springer-Verlag.
- Langheinrich M. (2005). *Personal Privacy in Ubiquitous Computing - Tools and System Support*. Ph.D. thesis, ETH (Zurich).
- Laplante P.A. (2007). *What Every Engineer Should Know about Software Engineering*.
- Latour B. (1985). « Les vues de l'esprit, une introduction à l'anthropologie des sciences et des techniques », *Culture technique*, no° 14, p. 4-30.
- Latour B. (1987). *Science in Action. How to follow scientists and engineers through society*, Cambridge, Harvard University Press.
- Latour B. (1991). *Nous n'avons jamais été modernes. Essai d'anthropologie symétrique.*, Paris, La Découverte.
- Latour B. (2005). *Changer la société. Refaire de la sociologie*, Paris La Découverte.
- Latour B. (2005). « From Realpolitik to Dingpolitik or How to Make Things Public », in Latour, B. et Weibel, P. (éd.) (2005). *Making Things Public. Atmospheres of Democracy*, Cambridge, MA, MIT Press, p. 14-43.
- Latour B. (2006). « Les "Vues" de l'Esprit" Une introduction à l'anthropologie des sciences et des techniques », in Akrich, M., Callon, M. et Latour, B. (éd.) (2006). *Sociologie de la traduction. Textes fondateurs*, Paris, Ecole des Mines
- Latour B. et Callon M. (éd.) (1991) *La science telle qu'elle se fait. Anthologie de la sociologie des sciences de langue anglaise*. Paris, La Découverte.



- Latour B. et Woolgar S. (1979). *Laboratory Life: The Social Construction of Scientific Facts* Beverly Hills, Sage Publications.
- Lave J. et Wenger E. (1991). *Situated Learning: Legitimate Peripheral Participation*, Cambridge, Cambridge University Press.
- Law J. (2004). *After Method: Mess in social Science Research*, London, Routledge.
- Law J. et Callon M. (1992). « The Life and Death of an Aircraft: A Network Analysis of Technical Change », in Bijker, W. et Law, J. (éd.) (1992). *Shaping TEchnology/Building Society*, Cambridge, London, The MIT Press, p. 21-52.
- Law J. et Mol A. (éd.) (2002) *Complexities. Social Studies of Knowledge Practices*. Durham, Duke University Press.
- Le Marec J. (2001). « L'usage et ses modèles : quelques réflexions méthodologiques », *Spirales*, no° 28, p. 105-122.
- Le Marec J. (2002). *Ce que le "terrain" fait aux concepts : vers une théorie des composites*. Habilitation à diriger des recherches, Université de Paris VII (Paris).
- Le Marec J. (2004). « Usages : pratiques de recherche et théorie des pratiques », *Hermès*, no° 38, p. 141-147.
- Le Marec J. et Babou I. (2003). « De l'étude des usages à une théorie des "composites": objets, relations et normes en bibliothèque », in Souchier, E., Jeanneret, Y. et Le Marec, J. (éd.) (2003). *Lire, écrire, récrire - objets, signes et pratiques des médias informatisés*, Paris, BPI, p. 233-299.
- Le Masson P., Hatchuel A. et Weil B. (2006). *Les processus d'innovation: conception innovante et croissance des entreprises*, Paris, Lavoisier.
- Lederer S. (2003). *Designing Disclosure : Interactive Personal Privacy at the Dawn of Ubiquitous Computing*. . M.S. report, Computer Science Division, University of California (Berkeley).
- Lee C., P (2007). « Boundary Negotiating Artifacts: Unbinding the Routine of Boundary Objects and Embracing Chaos in Collaborative Work », *Comput. Supported Coop. Work*, vol. 16, no° 3, p. 307-339.
- Légrand M. (2004). « L'expertise du sociologue: engagement et accompagnement du changement », in Légrand, M. et Vrancken, D. (éd.) (2004). *L'expertise du sociologue*, Paris, L'Harmattan, p. 81-142.
- Légrand M. et Vrancken D. (éd.) (2004) *L'expertise du sociologue*. Paris, L'Harmattan.
- Lemieux C. (2010). *La sociologie sur le vif*, Paris, Presses des mines.
- Leysia P. et Paul D. (2003). « Unpacking "privacy" for a networked world ». *Proceedings of the SIGCHI conference on Human factors in computing systems*, Ft. Lauderdale, Florida, USA, ACM.
- Lima L. (2009). « Les frontières de l'expertise », *Cahiers internationaux de sociologie*, vol. 1, no° 126, p. 149-155.
- Ljungbald S. (2008). *Beyond Users: Grounding Technology in Experience*. Doctoral Thesis, Dept. of Computer and Systems Sciences, Stockholm University (Stockholm).
- Lloyd P. (2000). « Storytelling and the development of discourse in the engineering design process », *Design Studies*, vol. 21, no° 4, p. 357-373.
- Löwgren J. et Stolterman R. (2004). *Thoughtful Interaction Design: A Design Perspective of Information Technology*, Cambridge, Massachusetts, MIT Press.
- Mackay H., Carne C., Beynon-Davies P. et Tudhope D. (2000). « Reconfiguring the User: Using Rapid Application Development », *Social Studies of Science*, vol. 30, no° 5, p. 737-757.
- MacKenzie D. et Wajcman J. (1999). « Introductory essay: the social shaping of technology », in MacKenzie, D. et Wajcman, J.e. (éd.) (1999). *The Social Shaping of Technology*, Buckingham, Open University Press, p. 3-27.

- Madlmayr G., Ecker J., Langer J. et Scharinger J. (2008). « Near Field Communication : State of Standardization », *First International Conference on The Internet of Things, IOT 2008 Workshops*.
- Maffesoli M. (2000). *L'instant éternel. Le retour du tragique dans les sociétés postmodernes*, Paris, Denoël.
- March J.G. (1991). « Exploration and exploitation in organizational learning », *Organization Science*, vol. 2, no° 1, p. 71-87.
- Martin D., Rooksby J. et Rouncefield M. (2007). « Users as contextual features of software product development and testing ». *Proceedings of the 2007 international ACM conference on Supporting group work*, Sanibel Island, Florida, USA, ACM.
- Matalon B. et Ghiglione R. (1998). *Les enquêtes sociologiques. Théories et pratique*, Paris, Armand Colin.
- Mercier A. (2009). « La vraisemblance : état de la question historique et théorique », *Temps Zéro*, no° 2.
- Mitchell C.T. (1993). *Redefining designing: from form to experience*, New York, Van Nostrand Reinhold.
- Morand P. et Manceau D. (2009) *Pour une nouvelle vision de l'innovation*. Paris, ESCP-EAP.
- Moscovici S. et Pérez J.-A. (2003). « La méthode expérimentale », in Moscovici, S. et Buschini, F. (éd.) (2003). *Les méthodes en sciences humaines*, Paris, PUF, p. 59-84.
- Nattiez J.-J. (1987). *Musicologie générale et sémiologie*, Paris, Bourgois.
- Navarro O., Forest F., Lavoisy O. et Chanal V. (2009) *L'utilisation du scénario dans le processus d'innovation. Une lecture pluridisciplinaire*. Grenoble, Umanlab.
- Nielsen L. (2002). « From user to character: an investigation into user-descriptions in scenarios ». *Proceedings of the 4th conference on Designing interactive systems: processes, practices, methods, and techniques*, London, England, ACM.
- Nielsen L. (2004). "Engaging Personas and Narrative Scenarios." Retrieved 15/02/2008, 2008, url: [ep.lib.cbs.dk/download/ISBN/x656444362.pdf](http://ep.lib.cbs.dk/download/ISBN/x656444362.pdf).
- Nizet J. et Rigaux N. (2005). *La sociologie de Erving Goffman*, Paris La Découverte.
- Norman D. (1993). *Things that make us smart*, Addison-Wesley.
- Norman D. (2004). *Emotional Design: Why We Love (Or Hate) Everyday Things*, New York, Basic Books.
- Nutch F. (1996). « Gadgets, Gizmos, and Instruments: Science for the Tinkering », *Science, Technology & Human Values*, vol. 21, no° 2, p. 214-228.
- OCDE (2003) *Manuel de Frascati 2002. Méthode type proposée pour les enquêtes sur la recherche et le développement expérimental*, OCDE.
- OCDE (2007) *Perspective de la science, de la technologie et de l'industrie de l'OCDE (synthèse)*. Paris, OCDE.
- Orlikowski W., J. et Gash D., C. (1994). « Technological frames: making sense of information technology in organizations », *ACM Trans. Inf. Syst.*, vol. 12, no° 2, p. 174-207.
- Osimo D. (2005). « Interview with Prof. Roger Silverstone, Professor of Media and Communications », *Communications & strategies*, no° 59, p. 101-112.
- Oudshoorn N. et Pinch T. (2003). « How Users and Non-Users Matter », in Oudshoorn, N. et Pinch, T. (éd.) (2003). *How Users Matter. The Co-Construction of Users and Technology*, Cambridge, London, MIT Press, p. 1-25.
- Oudshoorn N. et Pinch T. (2005). « How Users and Non-Users Matter » (2005). *How Users Matter. The Co-Construction of Users and Technology*, MIT Press, p. 1-25.
- Oudshoorn N., Rommes E. et Stienstra M. (2004). « Configuring the User as Everybody: Gender and Design Cultures in Information and Communication Technologies », *Science, Technology, & Human Values*, vol. 29, no° 1, p. 30-63.

- Palen L. et Dourish P. (2003). « Unpacking "privacy" for a networked world ». *Proceedings of the SIGCHI conference on Human factors in computing systems*, Ft. Lauderdale, Florida, USA, ACM.
- Passeron J.C. (1995). « L'espace mental de l'enquête », *Enquête*, no° 1.
- Peneff J. (1996). « Les débuts de l'observation participante ou les premiers sociologues en usine », *Sociologie du travail*, vol. 38, no° 1.
- Peretz H. (2004). *L'observation*, Paris, La Découverte.
- Pestre D. (1997). « La production de savoirs entre académies et marché. Une relecture historique du livre *The new production of knowledge*, édité par M. Gibbons », *Revue d'Economie Industrielle*, vol. 79, no° 1, p. 163-174.
- Petersen M.G., Luvigsen M., Jensen H.F. et Thomsen A. (2004). « Embracing Values in Designing Domestic Technologies », *Proceedings of ECCE 2004*.
- Phillips J. (2006). « Agencement/Assemblage », *Theory, Culture & Society*, vol. 23, no° 10, p. 108-109.
- Pinch T. (1993). « Do Not Despair: There Is Life After Constructivism », *Science, Technology & Human Values*, vol. 18, no° 1, p. 113-138.
- Pinch T. (1993). « Testing - One, Two, Three...Testing! : toward a sociology of testing », *Science, Technology and Human values*, vol. 18, no° 1, p. 25-41.
- Pinch T. (2003). « Giving birth to New Users : How the Minimoog Was Sold to Rock and Roll », in Oudshoorn, N. et Pinch, T. (éd.) (2003). *How users matter. The co-construction of users and technologies*, Cambridge, London, The MIT Press, p. 247-270.
- Pinch T. et Bijker W.E. (1989). « The social construction of facts and artifacts : or how the sociology of science and the sociology of technology might benefit each other », in Bijker, W.E., Hugues, T.P. et Pinch, T. (éd.) (1989). *The social construction of technological systems. New directions in the sociology and history of technology*, Cambridge, London, The MIT Press, p. 17-50.
- Pine B.J.I. et Gilmore J.H. (1998). « Welcome to the Experience Economy », *Harvard Business Review*, no° July-August 1998, p. 97-105.
- Pirou O. (2006). *La face cachée de la sociologie. A la découverte des sociologues praticiens*, Paris, Belin.
- Pirou O. (2008). « Le nouveau tournant de la sociologie en France dans les années 2000 », *Sociologies Pratiques*, no° 16, p. 123-130.
- Preece J., Rogers Y. et Sharp H. (2002). *Interaction Design: Beyond Human-Computer Interaction*, Wiley.
- Quéré L. (1992). « Espace public et communication: remarques sur l'hybridation des machines et des valeurs », in Chambat, P. (éd.) (1992). *Communication et lien social: usages des machines à communiquer [Actes du Colloque "Machines à communiquer", Paris-La Villette, 1991]*, Paris, Editions Descartes.
- Radder H. (1996). *In and about the world: Philosophical studies of science and technology*, Albany, State University of New York Press.
- Raitila V.-J. (2007). « Tag, you're it - NFC in a home environment », in Ylä-Jääski, A. et Takkinen, L. (éd.). *Seminar on Internetworking*, Helsinki, Helsinki University of Technology.
- Redström J. (2006). « Towards user design? On the shift from object to user as the subject of design », *Design Studies*, vol. 27, no° 2, p. 123-139.
- Reger G. (2001). « Technology Foresight in Companies: From an Indicator to a Network and Process Perspective », *Technology Analysis and Strategic Management*, vol. 13, no° 4, p. 533-553.
- Reichenbach H. (1938). *Experience and Prediction*, Chicago, University of Chicago Press.

- Reid S.E. et de Brentani U. (2004). « The Fuzzy Front End of New Product Development for Discontinuous Innovations: A Theoretical Model », *Journal of Product Innovation Management*, vol. 21, p. 170-184.
- Rip A. (1994). « The Republik of Science in the 1990 », *Higher Education*, vol. 28, no° 1.
- Rip A., Misa T.J. et Schot J. (éd.) (1995) *Managing Technology in Society. The Approach of Constructive Technology Assessment*. London, Pinter.
- Rogers Y. (1997). « Reconfiguring the Social Scientist: Shifting From Telling Designers What to Do to Getting More Involved », in Bowker, G., Star, S.L., Turner, W. et Gasser, L. (éd.) (1997). *Social Science, Technical Systems, and Cooperative Work: Beyond the Great Divide*, Lawrence Erlbaum Associates, p. 57-78.
- Rosenberg N. (1976). « On Technological Expectations », *The Economic Journal*, vol. 86, no° 343, p. 523-535.
- Salmon C. (2007). *Storytelling. La machine à fabriquer des histoires et à formater les esprits.*, Paris, Les éditions de minuit.
- Samarajiva R. (2001). « Interactivity As Though Privacy Mattered », in Agre, P.E. et Rotenberg, M. (éd.) (2001). *Technology and Privacy: The New Landscape*, The MIT Press, p. 277-310.
- Sanders E.B.-N. (2002). « From user-centered to participatory design approaches », in Frascara, J. (éd.) (2002). *Design and the Social Sciences: Making Connections*, London, Taylor & Francis, p. 1-8.
- Schmidt K. et Bannon L. (1992). « Taking CSCW Seriously: Supporting Articulation Work », *Computer Supported Cooperative Work (CSCW): An International Journal*, vol. 1, p. 7-41.
- Schmidt K. et Bannon L. (1992). « Taking CSCW seriously: Supporting articulation work », *Comput. Supported Coop. Work*, no° 1, p. 7-40.
- Schön D. (1992). « Designing as Reflective Conversation with the Materials of a Design Situation », *Knowledge-Based Systems*, no° 5, p. 3-14.
- Schot J. et Albert de la Bruheze A. (2003). « The Medicated Design of Products, Consumption, and Consumers in the Twentieth Century », in Oudshoorn, N. et Pinch, T. (éd.) (2003). *How users matter. The co-construction of users and technologies*, Cambridge, London, The MIT Press, p. 229-246.
- Seago A. et Dunne A. (1999). « New methodologies in art and design research: the object as discourse », *Design Issues*, vol. 15, no° 2, p. 11-18.
- Segrestin D. (2010). "La contribution des sociologues au génie industriel grenoblois." 2010, url: <http://genie-industriel.grenoble-inp.fr/20-ans/la-contribution-des-sociologues-au-genie-industriel-grenoblois-313267.kjsp>.
- Sengers P. et Gaver B. (2006). « Staying open to interpretation: engaging multiple meanings in design and evaluation ». *Proceedings of the 6th conference on Designing Interactive systems*, University Park, PA, USA, ACM.
- Shapiro D. (1994). « The limits of ethnography: combining social sciences for CSCW ». *Proceedings of the 1994 ACM conference on Computer supported cooperative work*, Chapel Hill, North Carolina, United States, ACM.
- Sharrock W. et Button G. (1997). « Engineering Investigations: Practical Sociological Reasoning in the Work of Engineers », in Bowker, G., Star, S.L., Turner, W. et Gasser, L. (éd.) (1997). *Social Science, Technical Systems, and Cooperative Work: Beyond the Great Divide*, Lawrence Erlbaum Associates, p. 79-104.
- Shinn T. (2000). « Axes thématiques et marchés de diffusion - La science en France, 1975-1999 », *Sociologie et sociétés*, vol. XXXII, no° 1, p. 43-69.
- Siira E. et Haiko J. (2007). « Experiences from Near-Field Communication (NFC) in a Meal Service System », *RFID Eurasia*.
- Simon H.A. (1960). *The New Science of Management Decision*, Harper & Row, New York.

- Siponen M., T. et Oinas-Kukkonen H. (2007). « A review of information security issues and respective research contributions », *SIGMIS Database*, vol. 38, no° 1, p. 60-80.
- Sirey B. (2007). « La notion de "privacy" au coeur des pratiques de consommation ». *6ème Journées Normandes de Recherche sur la Consommation : Société et consommations*, Rouen, Groupes ESC Rouen.
- Sismondo S. (2004). *An Introduction to Science and Technology Studies*, Oxford, Blackwell.
- Slaughter S. (1993). « Innovation and learning during implementation: a comparison of user and manufacturer innovations », *Research Policy*, vol. 22, no° 1, p. 81-95.
- Smith P.G. et Reinertsen D.G. (1995). *Developing Products in Half the Time*, New York, John Wiley & Sons.
- Sorensen K.H. (2009). « The Role of Social Science in Engineering », in Gabbay, D.M., Meijers, A. et Woods, J. (éd.) (2009). *Handbook of the Philosophy of Science. Philosophy of Technology and Engineering Sciences*, Burlington, MA, Elsevier, p. 93-116.
- Stewart J. et Claeys L. (2009). « Problems and opportunities of interdisciplinary work involving users in speculative research for innovation of novel ICT applications », *The Good, The Bad and The Challenging. The user and the future of information and communication technologies*, Copenhagen.
- Storm G. (2003). « Perception of Human-centered Stories and Technical Descriptions when Analyzing and Negotiating Requirements », *Proceedings of Human-Computer Interaction Interact'03*, IOS Press Netherlands.
- Strauss A.L. (1988). « The Articulation of Project Work: An Organizational Process », *The Sociological Quarterly*, vol. 29, p. 163-178.
- Subrahmanian E., Monarch I., Konda S., et al. (2003). « Boundary Objects and Prototypes at the Interfaces of Engineering Design », *Comput. Supported Coop. Work*, vol. 12, no° 2, p. 185-203.
- Suchman L. (1987). *Plans and Situated Actions : The Problem of Human-Machine Communication*, New York, Cambridge University Press.
- Tang J.C. (1991). « Findings from observational studies of collaborative work », *International Journal of Man Machine Studies*, vol. 34, no° 2, p. 143-160.
- Tarde G. (1901). « L'opinion et la foule », Tremblay, Jean-Marie.
- Teil G. (2010). « Arbitrer la présence des objets en société », in RT11, e.a.d.u.e.d.l.c.s.l.éd.l.A. (éd.), Paris.
- Thévenot L. (1986). « Les investissements de forme », in Thévenot, L. (éd.) (1986). *Conventions économiques*, Paris, Presses Universitaires de France, p. 21-71.
- Tognazzini B. (1994). « The "Starfire" video prototype project - a case history », *Proceedings of the SIGCHI conference on Human factors in computing systems*, p. 99-105.
- Trépos J.-Y. (1996). *La sociologie de l'expertise*, Paris, Presses Universitaires de France.
- Trépos J.-Y. (2001). « L'expertise sociologique ou le complexe de l'albatros », in Vrancken, D. et Kutty, O. (éd.) (2001). *La sociologie et l'intervention. Enjeux et perspectives*, Bruxelles, De Boeck, p. 211-242.
- Trépos J.-Y. (2001). « Les expertises: entre événement et équipement », in Damien, R. (éd.) (2001). *L'expertise*, Paris, Presses Universitaires Franc-Comtoises, p. 99-126.
- Trompette P. et Blanco E. (2009). « Projeter sans fermer la carrière sociale des innovations », in Chalas, Y., Gilbert, C. et Vinck, D. (éd.) (2009). *Comment les acteurs s'arrangent avec l'incertitude*, Paris, Editions des archives contemporaines, p. 97-116.
- Trompette P. et Vinck D. (2009). « Retour sur la notion d'objet-frontière », *Revue d'Anthropologie des Connaissances* vol. 3, no° 1, p. 5-27.
- Tyldesley D.A. (1988). « Employing usability engineering in the development of office products », *The Computer Journal*, vol. 31, no° 5, p. 431-436.

- Un S. et Price N. (2007). « Bridging the gap between technological possibilities and people: Involving people in the early phases of technology development », *Technological Forecasting and Social Change*, no° 74, p. 1758-1772.
- Vaajakallio K. et Mattelmäki T. (2007). « Collaborative design exploration: envisioning future practices with make tools », *Proceedings of the 2007 conference on Designing pleasurable products and interfaces*, Helsinki, Finland, ACM.
- van Kammen J. (1999). « Representing Users' Bodies: The Gendered Development of Anti-Fertility Vaccines », *Science, Technology & Human Values*, vol. 24, no° 3, p. 317-337.
- van Kammen J. (2003). « Who represents the users? Critical encounters between Women's Health Advocates and Scientists in Contraceptive R&D », in Oudshoorn, N. et Pinch, T. (éd.) (2003). *How users matter. The co-construction of users and technologies.*, Cambridge, London, The MIT Press, p. 151-172.
- Vassilis K. et Eamonn O.N. (2007). « NFC on Mobile Phones: Issues, Lessons and Future Research », *Proceedings of the Fifth IEEE International Conference on Pervasive Computing and Communications Workshops*, IEEE Computer Society.
- Vedel T. (1994). « Sociologie des innovations technologiques des usagers: introduction à une socio-politique des usages », in Vitalis, A. (éd.) (1994). *Médias et nouvelles technologies. Pour une socio-politique des usages*, Rennes, Apogée, p. 13-43.
- Verchère C. et Anjembe E. (2010). « De la difficulté de fabriquer des objets-frontières. Le cas d'un projet de conception exploratoire », *Revue d'Anthropologie des Connaissances*, vol. 4, no° 1, p. 36-64.
- Vergragt P.J. (1988). « The Social Shaping of Industrial Innovations », *Social Studies of Science*, vol. 18, no° 3, p. 483-513.
- Vinck D. (1995). « Mediating and Commissioning Objects in the Sociotechnical Process of Product Design: a conceptual approach », in Maclean, D., Saviotti, P. et Vinck, D. (éd.) (1995). *Designs, Networks, Strategies*, Bruxelles, EC Directorate General Science R&D.
- Vinck D. (éd.) (1999) *Ingénieurs au quotidien. Ethnographie de l'activité de conception et d'innovation*. Grenoble, PUG.
- Vinck D. (2000). *Pratiques de l'interdisciplinarité. Mutation des sciences, de l'industrie et de l'enseignement*, Grenoble, PUG.
- Vinck D. (2003). « Epilogue: Approaches to the Ethnography of Technologies », in Vinck, D. (éd.) (2003). *Everyday Engineering: An Ethnography of Design and Innovation*, Cambridge, MA, MIT, p. 203-226.
- Vinck D. (éd.) (2003) *Everyday Engineering*. Boston, MA, MIT Press.
- Vinck D. (2007). *Sciences et société. sociologie du travail scientifique*, Paris, A. Colin.
- Vinck D. (2009). « De l'objet intermédiaire à l'objet-frontière. Vers la prise en compte du travail d'équipement », *Revue d'anthropologie des connaissances*, vol. 3, no° 1, p. 51-72.
- Vinck D. et Laureillard P. (1996). « Coordination par les objets dans les processus de conception », *Journées CSI "Représenter, Attribuer, Coordonner*, Paris.
- Vitalis A. (éd.) (1994) *Médias et nouvelles technologies. Pour une socio-politique des usages*. Rennes, Editions Apogée.
- von Hippel E. (1976). « The dominant role of users in the scientific instrument innovation process », *Research Policy*, vol. 5, no° 3, p. 212-239.
- von Hippel E. (1994). « "Sticky Information" and the Locus of Problem Solving: Implications for Innovation », *Management Science*, vol. 40, no° 4, p. 429-439.
- von Hippel E. et Tyre M.J. (1995). « How learning by doing is done: problem identification in novel process equipment », *Research Policy*, vol. 24, no° 1, p. 1-12.

- Vrancken D. (2004). « Les fondements procéduraux de l'expertise sociologie », in Legrand, M. et Vrancken, D. (éd.) (2004). *L'expertise du sociologue*, Paris, L'Harmattan, p. 19-55.
- Vrancken D. et Kutty O. (éd.) (2000) *La sociologie et l'intervention. Enjeux et perspectives*. Bruxelles, De Boeck.
- Wagner I. (1997). « On Multidisciplinary Grounds: Interpretation Versus Design Work », in Bowker, G., Star, S.L., Turner, W. et Gasser, L. (éd.) (1997). *Social Science, Technical Systems, and Cooperative Work: Beyond the Great Divide*, Lawrence Erlbaum Associates, p. 415-432.
- Webb B. (1996). « The role of users in interactive system design: When computers are theatre, do we want the audience to write the script ? », *Behaviour and Information Technology*, vol. 15, p. 76-83.
- Wenger E. (1998). *Communities of Practice*, New York, NY, Cambridge University Press.
- Winner L. (1980). « Do Artefacts Have Politics? », *Daedalus*, vol. 109, p. 121-136.
- Winner L. (1993). « Upon opening the black box and finding it empty: social constructivism and the philosophy of technology », *Science, Technology & Human Values*, vol. 18, no° 3, p. 362-378.
- Woolgar S. (1991). « Configuring the user. The case of usability trials », in Law, J. (éd.) (1991). *A Sociology of Monsters: Essays on Power, Technology and Domination*, London, Routledge, p. 57-102.
- Woolgar S. (1991). « The Turn to Technology in Social Studies of Science », *Science, Technology & Human Values*, vol. 16, no° 1, p. 20-50.
- Woolgar S. (1994). « Rethinking Requirements Analysis: Some Implications of Recent Research into Producer Consumer Relationships in IT Development », in Jirotko, M. et Goguen, J. (éd.) (1994). *Requirements Analysis: Social and Technical Issues*, London, p. 201-216.

# **Annexes**



## **Annexe 1.**

# **Objets mobilisés durant la conception du scénario**

Figure42



## Contactless Privacy Manager



A third device, the CPM (in blue), can enable to protect against unsolicited readings and to monitor them

- ☐ The CPM works like a blocker tag at the singulation protocol level
- ☐ Time-slotted probabilistic singulation protocols were used because they are the most common in 13.56 MHz standards
- ☐ The CPM creates a collision in the time-slot where an unknown or dangerous tag answers

© CEA 2008. Tous droits réservés.  
Toute reproduction totale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est interdite sans l'autorisation écrite préalable du CEA.  
All rights reserved. Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA.

O. SAVRY Kick off COPRIM 1/02/2008 | 22

threats	attacks	risks	control the attack	possible scenario	improvised standards	mount countermeasures	net. of countermeasures
Threat of eavesdropping	Man-in-the-middle						
	jamming						
	RFID guard						
	forward relay						
	wireless and wireless						
Passive eavesdropping							
Active eavesdropping							
Disturbance							
Fault generation							
Wireless eavesdropping / dual mode / mobile							
Wireless eavesdropping / man-in-the-middle							
Wireless eavesdropping / substitution							

O.S. AVRY Kickoff COFRIN 1.02/2008 | 7

*Figure 44*



## Defining the privacy issue

Our goal is to analyse NFC-enhanced devices privacy related threats by identifying :

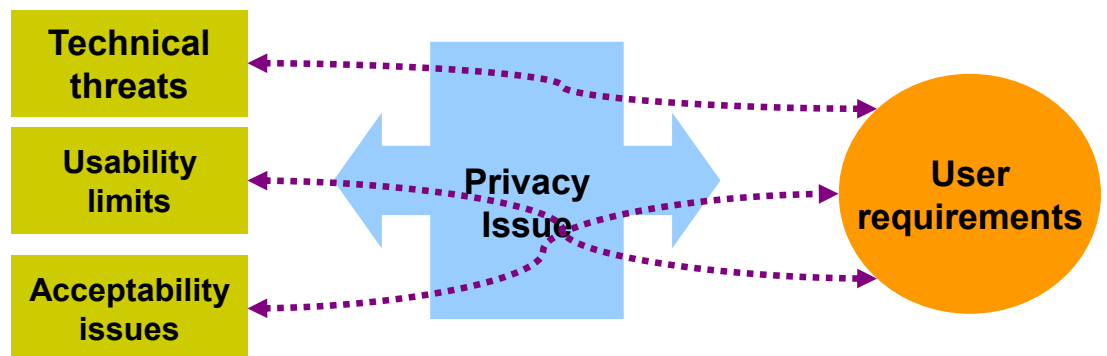


Figure45

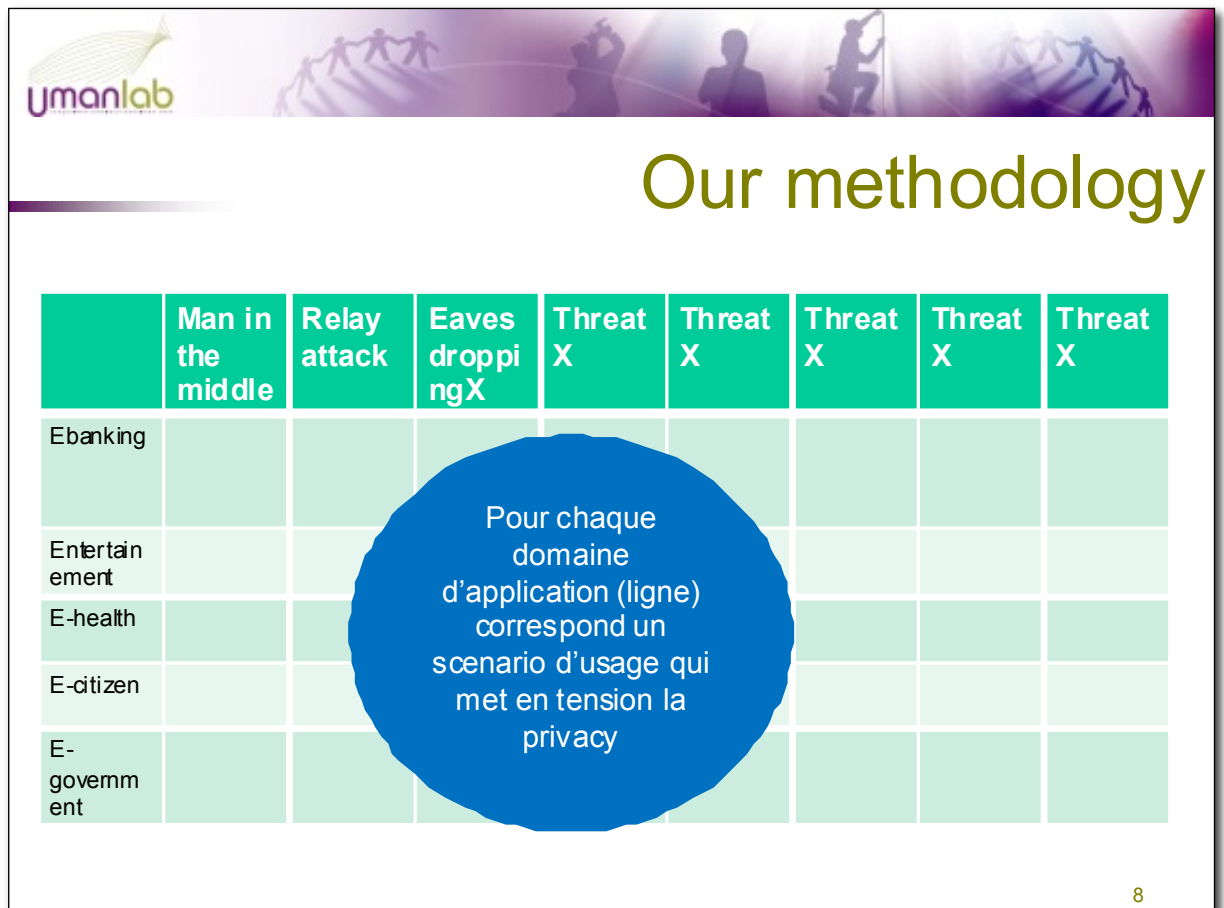


## Defining the privacy issue


Understanding privacy related issues from a HCI inspired framework (Lederer, 2003) :

- The privacy space is broken down into a **set of interdependent dimensions** that help defining a phenomenon's implications for privacy.
- These dimensions are *interdependent* and *flexible*. They are **System properties**, **Actor relations** and **Information types**.

Figure 46



**Figure 47**




## Projet ANR/TLCOM COPRIM

- ❑ Première analyse des scénarios menaces de la vie privée via le sans contact
- ❑ Aspect malveillant à l'origine (pas un pb de sûreté/sécurité de fonctionnement)
- ❑ Définition d'un scénario:
  - Attaquant: gain économique, fun, notoriété, ...
  - Domaine d'application (dont opérateur): bancaire, transport, fidélité, ....
  - La personne attaquée: utilisateur, opérateur, attaquant !!??
  - Objet attaqué: clés, algorithme, ...
  - Angle d'attaque: confidentialité, intégrité, disponibilité, détournement, usurpation,
  - Aspect de la vie privée ciblé: nom, agenda, photos, dossiers, droit d'accès à un service, un lieu géographique, à la mémoire en RD/WR, traçabilité: lieu et heure, ...
  - Méthode d'attaque
  - Difficulté de réalisation: compétence, délais de réalisation, coût, moyen d'attaques, déploiement des moyens d'attaques,
  - Aspect légal....
  - Aspect risque pour l'attaquant
  - Attaque unique ou répétitive ou de masse
  - Conséquences directes ou indirectes de l'attaque

© CEA 2006. Tous droits réservés.  
Toute reproduction totale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est interdite sans l'autorisation écrite préalable du CEA.  
All rights reserved. Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA.

F. Vacherand ConfCall 27 aout 2008 | 5

**Figure 48**



## Projet ANR/TLCOM COPRIM

- ❑ Première ébauche de critères de sélection des scénarios pertinents
- ❑ Identification et évaluation des différents critères
  - Gain final pour l'attaquant
  - Crainte pour l'utilisateur
  - Risque pour l'utilisateur
  - Conséquences
  - Difficulté du mode opératoire
  - Cout préparation attaque,
  - Cout contre-mesure
  - ....
- ❑ Définir une méthodologie de sélection des scénarios pertinents
  - Elaborer méthodologie de cotation pour l'indentification des priorités

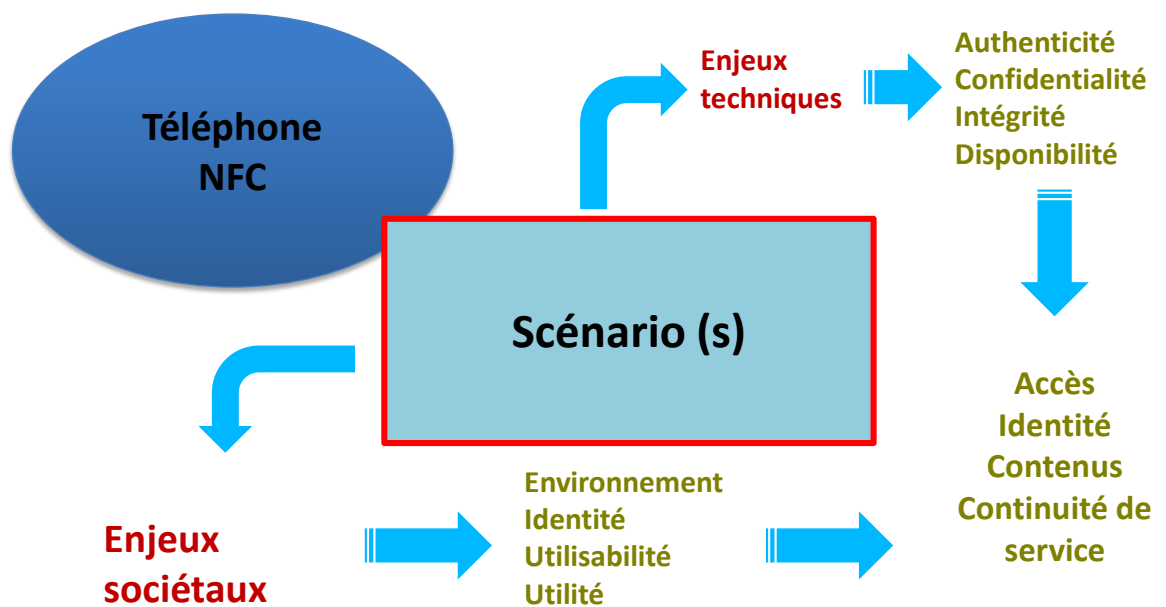
© CEA 2006. Tous droits réservés.  
Toute reproduction totale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est interdite sans l'autorisation écrite préalable du CEA.  
All rights reserved. Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA.

F. Vacherand ConfCallf 27 aout 2008 | 6



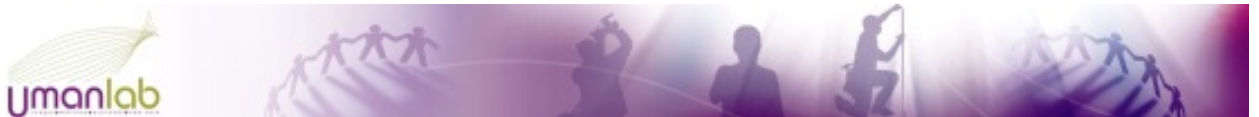
Figure49

## Choix d'un scénario



3

*Figure 50*



## Transport scenario *Characters*

- Julie : a teenager.
- Yves : Julie's grand-father.
- Charly1, Charly2, Charly3 : a herd of thugs.
- Bus Company.

Julie and Yves take the same bus, travelling together.

Figure 51



## Transport scenario - *Synopsis*

- 1/ Payment : Julie renews her monthly transport subscription at an automatic machine by using her mobile.
- 2/ Ticketing : Inside the bus, she validates her coupon by waving her mobile near the on-board reader.
- 3/ Contactless token : Julie points out an e-poster about a concert she's interested in. But this is too expensive. Yves quietly downloads the information via NFC (and books one seat for her via GSM/3G).
- 4/ P2P : Yves uploads the e-ticket to Julie's own mobile.

3

Figure 52



## Transport scenario

### *Eavesdropping attacks*

- 1/ Charly1 steals her bank references.
- 2/ Charly2 steals her ID for transport.
- 3/ Charly3 spies Yves downloading the URL (and learns that he's purchasing a ticket online).
- 4/ Charly3 duplicates the e-ticket.

Figure 53

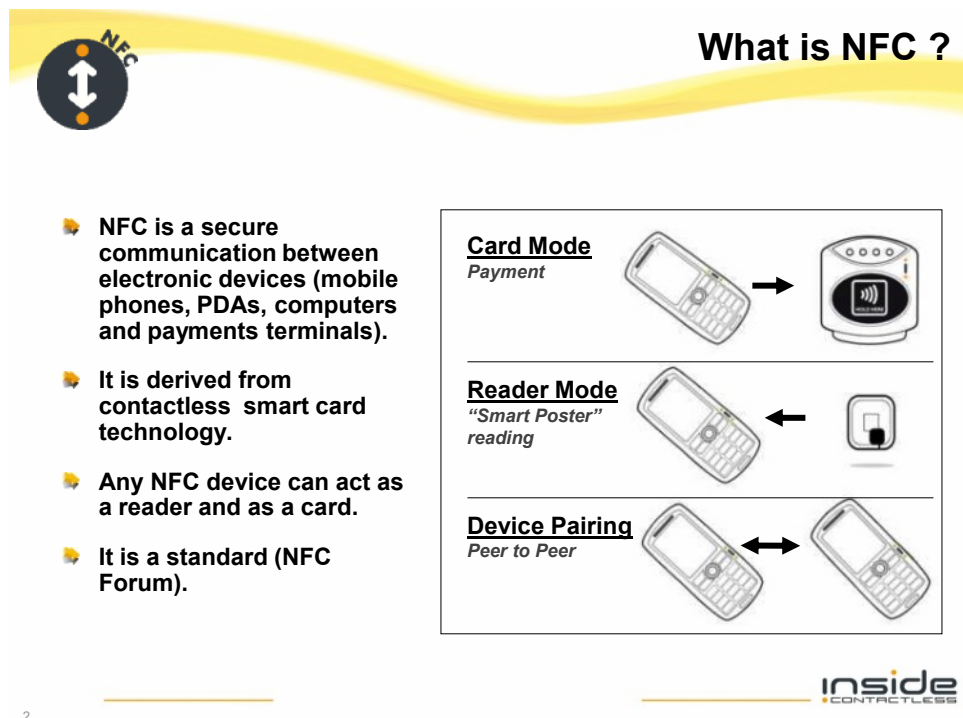
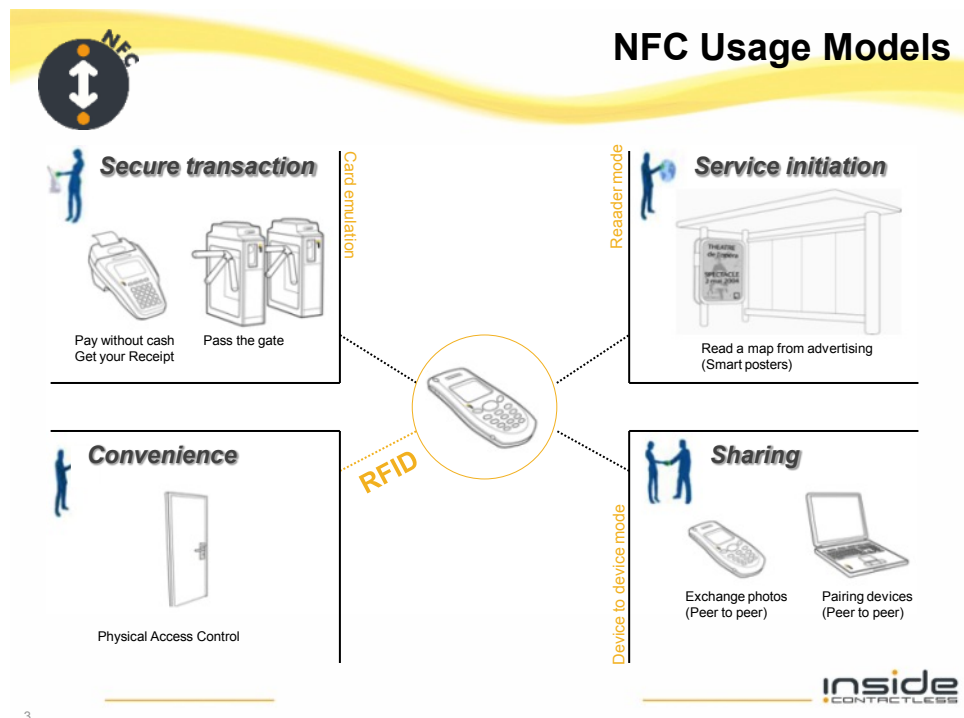


Figure 54



3

Figure 55



## Synopsis « Transport »

- **1/ Payment : Julie renews her monthly transport subscription at an automatic machine by using her mobile.**
- 2/ Ticketing : Inside the bus, she validates her coupon by waving her mobile near the on-board reader.
- 3/ Contactless token : Julie points out an e-poster about a concert she's interested in. But this is too expensive. Yves quietly downloads the information via NFC (and books one seat for her via GSM/3G).
- 4/ P2P : Yves uploads the e-ticket to Julie's own mobile.

3

Figure 56

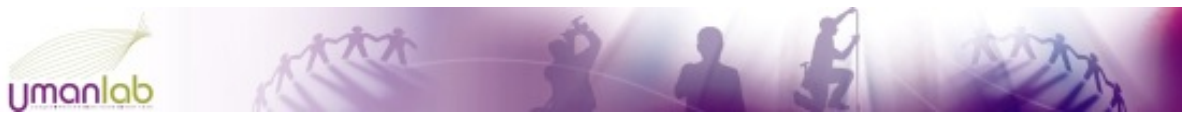


## « Attaque en relais »

« Payment »	Alice	Charlie 1	Charlie 2
Prologue	<p>1/ Alice achète un carnet de tickets en approchant son téléphone de la borne. Elle doit valider son achat par code PIN, puis elle range le téléphone dans son sac.</p> <p>2/ Puis, elle attend sur le quai bondé l'arrivée du tram.</p>	<p>1/ Charlie 1 espionne Alice et transmet son code (SMS, etc.) à Charlie 2.</p> <p>2/ Charlie 1 se met à 30 cm d'Alice. Il voit Charlie 2 qui est à quelques dizaines de mètres.</p>	<p>1/ Charlie note le code d'Alice.</p> <p>2/ Charlie 2 attend près de la borne, en surveillant <i>de visu</i> la scène.</p>
Attaque réussie		<p>2/ Le faux lecteur, porté par Charlie 1, lit la carte d'Alice sur le requête de Charlie 2.</p> <p>3/ L'attaque réussit.</p>	<p>2/ Charlie 2 se connecte à la borne avec sa fausse carte et, en même temps, il est en liaison radio avec le faux lecteur de Charlie 1.</p> <p>3/ Possédant le code Pin d'Alice, Charlie 2 est en mesure d'acheter une série de tickets en débitant le compte bancaire d'Alice. L'attaque réussit.</p>
Attaque échouée (cas 1)	<p>1/ Elle range le téléphone dans son sac.</p> <p>2/ Alors qu'elle va monter dans le tram, le téléphone d'Alice lui signale une demande de connexion (Hp, vibration, ...).</p> <p>3/ Elle refuse, sans même s'apercevoir de la présence de Charlie 1.</p>	<p>2/ Le faux lecteur, porté par Charlie 1, n'arrive pas à lire la carte d'Alice.</p> <p>3/ L'attaque donc échouée.</p>	<p>2/ Charlie 2 ne peut pas se connecter à la borne.</p> <p>3/ L'attaque donc échouée.</p>
Attaque échouée (cas 2)	<p>1/ Devant la borne, Alice initialise la fonction « NFC » de son téléphone. Après transaction, elle range le téléphone dans son sac en désactivant la fonction « NFC » de son téléphone.</p> <p>2/ Rien ne se passe.</p>	<p>2/ Le faux lecteur, porté par Charlie 1, n'arrive pas à lire la carte d'Alice.</p> <p>3/ L'attaque donc échouée.</p>	<p>2/ Charlie 2 ne peut pas se connecter à la borne.</p> <p>3/ L'attaque donc échouée.</p>



Figure 57



## Et le COPRIM ?

« COPRIM »	Initialisation	Interrogation	Validation
<b>Cas 1 :</b>  COPRIM « autonome »	Automatique par COPRIM	COPRIM interroge ALICE : « OK ? » ou « Pas OK ? ».  • Bip. • Vibration. • Animation à l'écran. • (...)	Par ALICE : elle valide ou non la transaction.  • Code ? • Bouton ? • Voix ? • Empreinte digitale ? • (...)
<b>Cas 2 :</b>  COPRIM « contrôlé »	Par ALICE : elle autorise ou pas la fonction « NFC »  • Code ? • Bouton ? • Voix ? • Empreinte digitale ? • (...)	Rien	Par ALICE : elle valide ou non la transaction.  • Code ? • Bouton ? • Voix ? • Empreinte digitale ? • (...)


### Commentaires :

- Au niveau de la conception : faut-il enfermer le COPRIM dans une boîte noire (non configuration par l'utilisateur) ?
- Au niveau de l'usage (Alice) : faut-il laisser le choix *a priori* (lorsqu'Alice sort de chez elle, par exemple) entre le cas 1 ou du cas 2 ?

Figure 58

### What is a security notion ?

- A security notion directly reflects a threat
- How to define a security notion  
Just specify:
  - An adversarial goal: what is the attacker trying to do ?
  - An attack model: what has the attacker access to ?
- There are several security notions  
each of which reflects a specific attack scenario

PRISM

4




Figure 59


## Security notions for COPRIM

○ Basic security notions

- Secrecy = passive/active authentication does not reveal  $\sigma$
- Forward secrecy = passive/active interaction does not reveal  $\sigma$  even if  $\pi$  known
- Password privacy = resistance to offline dictionary attacks on  $\pi$


○ More subtle security notions

- Untraceability = cannot trace chip identity afterwards
- Unlinkability = traces are unlinkable
- Non-transferability = terminal cannot prove transaction to third parties




PRISM

5



UNIVERSITÉ DE VERSAILLES  
SAINT-QUENTIN-EN-YVELINES

*Figure 60*



## Projet ANR/TLCOM COPRIM

- ☐ Document: Scénarios COPRIM (Anglais, Word Template (OS) Objectif final draft : fin avril 09)
- ☐ Proposition de structuration la table des matières
- ☐ Introduction
- ☐ Description générale des scénarios (UPMF)
  - Présentation des 4 cas + mettre en évidence l'aspect privacy » + pertinence (le pourquoi du choix fin fev 09)
- ☐ Description de chaque cas (une première boucle sur paiement fin fev 09: une deuxième boucle avec les 4 cas fin avril)
  - Protocole applicatif (Inside + UVSQ) + comm (LETI)
  - Attaque sur sans contact (Inside + UVSQ + LETI)
  - Analyse de risque pour pertinence et priorité des attaques à traiter dans ce cas (Critère sociologique puis critère technique)
- ☐ Conclusion

© CEA 2006. Tous droits réservés.  
Toute reproduction totale ou partielle sur quelque support que ce soit ou utilisation du contenu de ce document est interdite sans l'autorisation écrite préalable du CEA.  
All rights reserved. Any reproduction in whole or in part on any medium or use of the information contained herein is prohibited without the prior written consent of CEA.

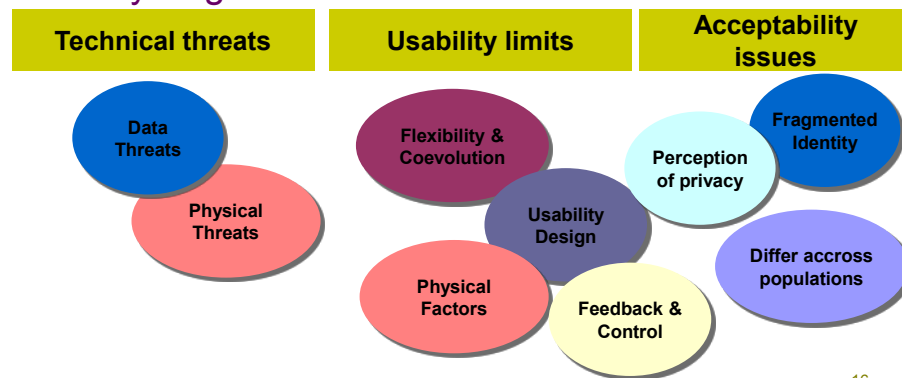
F. Vacherand Copil N2 COPRIM 5 sept 2008 | 12

Figure 61



## Tackling the privacy issue : *A multi factor perspective*

Each use case is analysed in regard to this  
analysis grid :



16

Figure 62

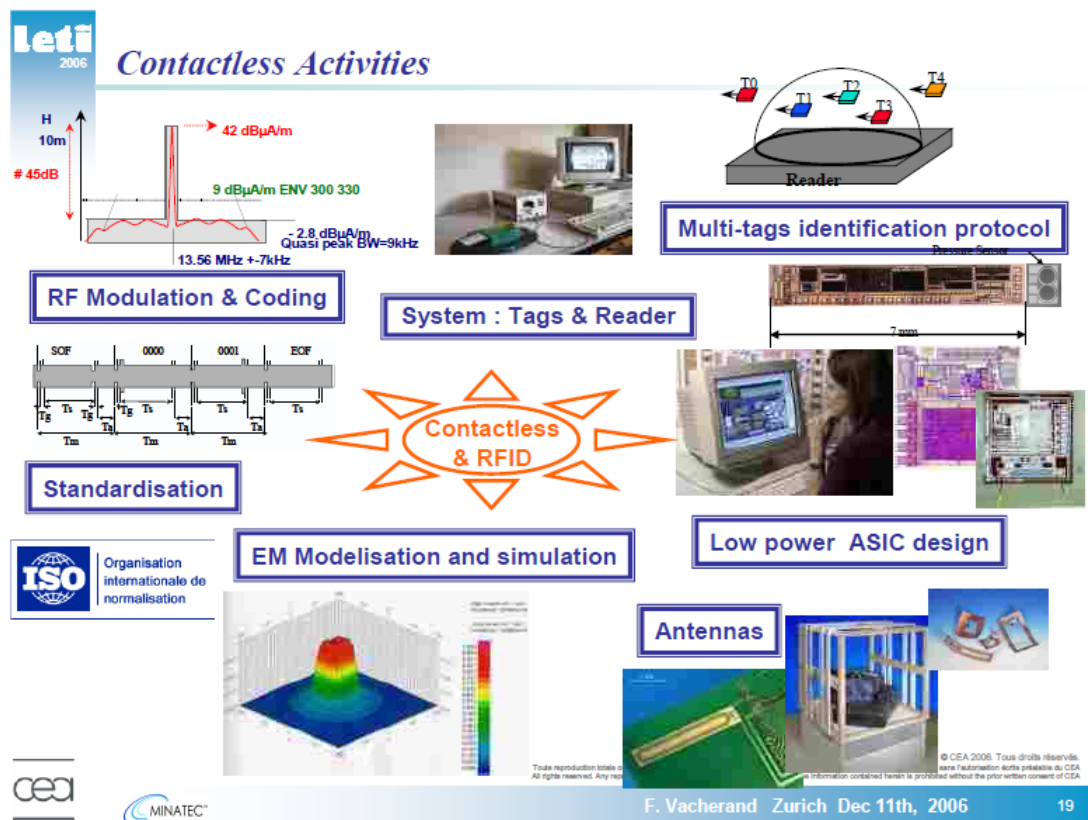


Figure 63

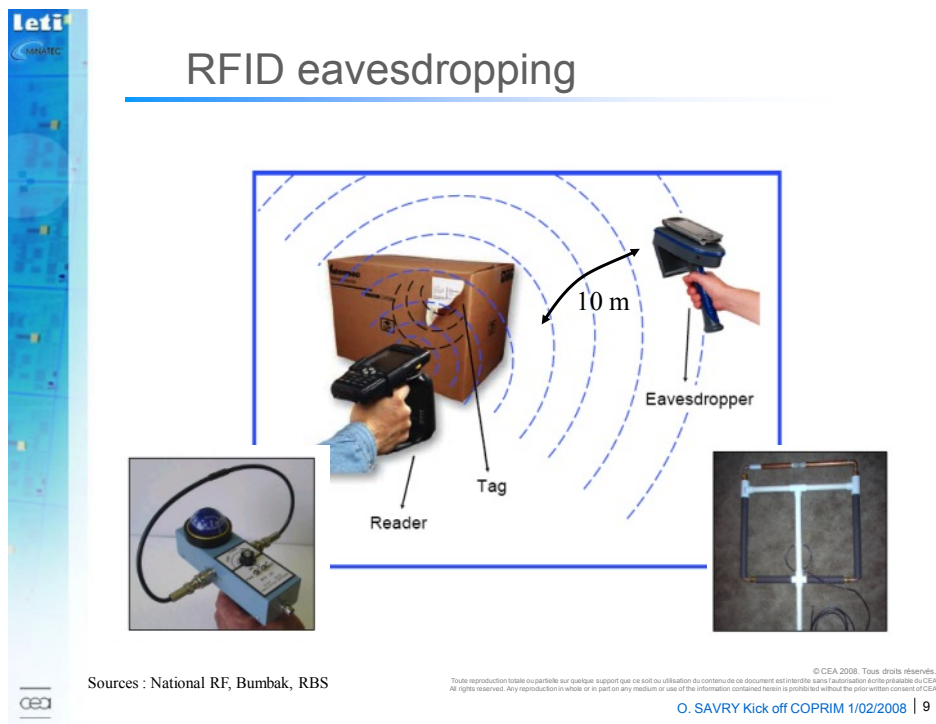
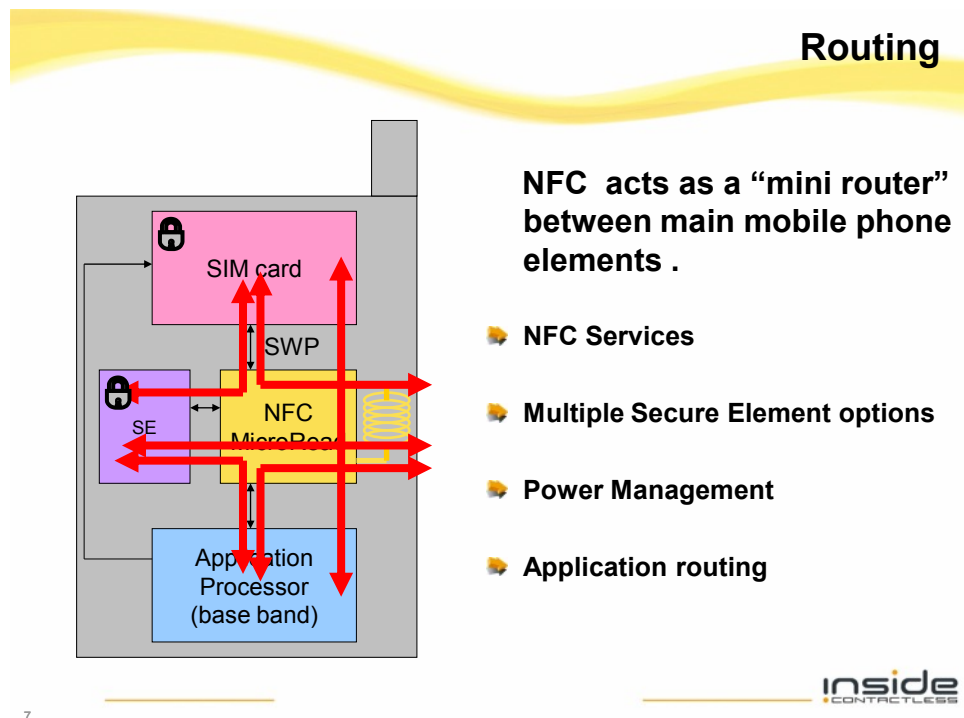


Figure 64



7



## **Annexe 2.**

### **State of the art NFC and Privacy**



State of the art : NFC and Privacy

Configuration réduite

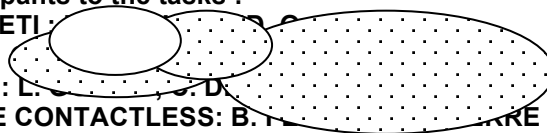
Participants to the tasks :

CEA LETI :

UPMF :

UVSQ : L.

INSIDE CONTACTLESS: B. T. KRE



**Classification to specify**

## **Summary**

During the last years, we attended to a fast deployment of contactless systems. RFID tags and contactless smartcards are now a part of our lives. Recently a new device has emerged : the NFC phone borrows this technology. Since those devices handle personal and confidential data, the citizen's privacy might be endangered.

This document presents the features of contactless systems particularly NFC and tries to show their impact on the society and on our privacy. The different threats are then introduced: eavesdropping, denial of service, skimming, relay attack, man in the middle attack, side channel attacks, destruction and DFA constitute an exhaustive survey. Facing this framework, security models are inferred and the different existing solutions are described ,

## **Keywords**

RFID, NFC, contactless, privacy, eavesdropping, skimming, relay attack, man in the middle attack, denial of service, side channel attack, DFA

COPRIM	31/01/09			334/556
Document	Date	Auteur	Version	Page

## **Table of contents**

<b>1</b>	<b><i>Introduction</i></b>	<b>338</b>
1.1	<b>Project Introduction (CEA)</b>	<b>338</b>
1.2	<b>Privacy, Society and new technologies (UPMF)</b>	<b>339</b>
1.2.1	A brief historical account of privacy	341
1.2.1.1	The individual's birth and the dawn of a concept	341
1.2.1.2	Information privacy, a concept that bolsters Privacy definition	343
1.2.2	The very contingency of a concept	346
1.2.2.1	Finding common points in contingency	346
1.2.2.2	The border paradigm: underlying the dynamic side of privacy contingency	349
1.3	<b>Privacy and RFID (CEA)</b>	<b>351</b>
1.3.1	Introduction of contactless systems	351
1.3.2	Comparing contactless cards with contact cards	351
1.3.3	Economical and Societal context and trusted computing	352
1.3.4	Security models for contactless cryptographic protocols	355
1.3.5	Objects concerned: tags, contactless cards, NFC phone	359
1.3.5.1	RFID tags	359
1.3.5.2	Contactless cards	359
1.3.5.3	NFC phone	359
1.3.6	Low Resources Devices and Security Issues	359
1.4	<b>Introduction to NFC (INSIDE)</b>	<b>360</b>
1.4.1	Description of NFC	360
1.4.2	Brief History of NFC	361
1.4.3	NFC Mobile Phone Architecture	362
1.4.4	Applications	363
<b>2</b>	<b><i>Threats on NFC</i></b>	<b>364</b>
2.1	<b>Current physical attacks on NFC-Systems</b>	<b>364</b>
2.1.1	Eavesdropping	364
2.1.2	Skimming	367
2.1.3	Denial of service	368
2.1.3.1	Interferences in the anti-collision protocols: blocker tag and RFID guardian	368
2.1.3.1.1	Anti-collision protocols	368
2.1.3.1.2	Deterministic protocol	368
2.1.3.1.3	Tree-walking example	370
2.1.3.1.4	Probabilistic protocol	371
2.1.3.1.5	Example of reader-to-tag dialogue	372

COPRIM	31/01/09			335/556
--------	----------	--	--	---------

2.1.3.1.6	The blocker tag	375
2.1.3.1.7	The RFID Guardian	375
2.1.3.2	Reader and card jamming	377
2.1.3.3	Shielding and using a Faraday cage	378
2.1.3.4	Viruses and worms	379
2.1.4	Relay Attack	380
2.1.5	“Man in the middle” attack	384
2.1.6	Side channel attacks on the contactless interface	384
2.1.6.1	Power Consumption Analysis	384
2.1.6.2	Simple Power Analysis	385
2.1.6.3	Differential Power Analysis	386
2.1.6.4	Electromagnetic Analysis	389
2.1.6.5	Radio Frequency Analysis	390
2.1.7	Differential Fault Analysis and Fault Injection Attacks	391
2.1.8	Attacks on multi interfaces smartcards	392
2.1.8.1	Coexistence of different interfaces	392
2.1.8.2	Crosstalking attack	393
2.1.9	Destruction	394
2.1.9.1	Material destruction	394
2.1.9.2	Software destruction	395
2.1.10	Counterfeiting, substitution and replay attack	395
<b>3</b>	<b><i>Designing for privacy : a social technical standpoint</i></b>	<b>396</b>
<b>3.1</b>	<b>Security, privacy and the technical device</b>	<b>399</b>
3.1.1	Understanding the links between security privacy and the technical device	399
3.1.2	How to Trust a sociotechnical order	404
<b>3.2</b>	<b>Some operational lessons for design</b>	<b>409</b>
<b>4</b>	<b><i>Existing solutions</i></b>	<b>413</b>
<b>4.1</b>	<b>Countermeasures on the physical layer</b>	<b>413</b>
4.1.1	The “Kill” Tag Approach	413
4.1.2	Optical Reading	413
4.1.3	The Faraday Cage	413
4.1.4	Active Jamming	414
4.1.5	Noisy Tags	414
4.1.6	The Blocker Tag	414
4.1.7	The RFID Guardian	414
<b>4.2</b>	<b>Solutions on the protocol level</b>	<b>415</b>
4.2.1	Distance bounding protocol (UVSQ)	415
4.2.1.1	Introduction	415
4.2.1.2	Known Protocols	415

4.2.1.2.1	Brands and Chaum [BC93].	415
4.2.1.2.2	Waters and Felten [WF03].	417
4.2.1.2.3	Sastry, Shankar and Wagner [SSW03].	417
4.2.1.2.4	Hancke et Kuhn [HK05].	418
4.2.1.2.5	Bussard and Bagga [BB05].	419
4.2.1.2.6	Reid <i>et al.</i> [RNTS07].	420
4.2.1.2.7	Capkum and Hubaux [CH06].	421
4.2.1.3	Discussion	422
<b>4.3</b>	<b>The MIFARE solution</b>	<b>422</b>
<b>5</b>	<b><i>Bibliography</i>.....</b>	<b>427</b>

## ■ Introduction

---

### ■ Project Introduction (CEA)

The fast deployment of contactless systems makes that they are already part of the electronic products used daily by millions of people. One can take as example the public transport domain. These devices represent a category of digital components which are at the base of the future Ambient Intelligence: smart cards and RFID tags. Starting from existing smart cards standards (ISO 14 443 and ISO 15 693), a generic standard grouping these standards and the most widespread contactless products of ISM band 13.56 MHz has emerged: the NFC standard (ECMA 340 & 352, ISO 18092). NFC stands for "Near Field Communication", i.e. for the products functioning in inductive coupling, and thus with short range contrary to wireless devices. Let us note that today this standard is in the course of deployment on the mobile phones. What all the more increases the diffusion and the use of this contactless technology.

However a certain concern arose from the users of the contactless technology concerning the protection of the private life. Indeed these contactless systems can be potentially the object of malicious actions trying to jeopardize the confidentiality of the exchanged data. Moreover the characteristic of the contactless objects is that these actions can take place without the owner of the object being informed, therefore without its awareness. Without protection measures the concept of Ambient Intelligence can trace somebody.

Contrary to the security problem of the contactless link which is related to the fight against the intentional economical fraud, the problem of protection of the private life relates to the handling of the personal data or revealing information not desired by its owner. To get a service one must reveal his identity to the operator who wishes him to protect his accesses. To be tracked permanently even to be plundered more or less involuntarily by the electronic devices related to the Ambient Intelligence raises another problem: be able to propose to the user a deprived sphere around him in order to isolate himself from the digital world and to keep its anonymity. It will have however to be taken care that this disconnection is not prone to cause situations of deny of service.

The main goal of the COPRIM project is to propose relevant and viable solutions from the economical point of view, in order to give again the full control to the user and by that to maintain the confidence which he carries to these electronic objects.

The project has 4 major axes of work:

- to propose technico-economical primitives of solutions of protection of the private life of the systems of t NFC type
- To give confidence to the user in the contactless products (NFC)
- to establish a business model for diffusion of the primitives of protection of the private life
- to validate on relevant scenarios these primitives of protection of the private life.

Technical challenges:

- Permanent monitoring of the electromagnetic environment at 13.56MHz (NFC)
- Detection of attempt of connection without the knowledge of the holder
- Management of physical and protocol barriers for the control of the access by the user
- Constraints due to the portable objects with low energy and processing resources

Expected results:

- Better vision of the needs for NFC systems in term of protection of the private life
- Compatibility of the protection measures of the private life with the security
- Reduction of the possibilities of malicious use of the functions of protection of the private life for deny of service
- Business model in relation to that of the NFC
- Maintenance of the confidence of the users in the contactless portable objects of the type NFC

## ■ Privacy, Society and new technologies (UPMF)

As acting participants in the design of a technical device, it has been clear to the sociologist team that the section dealing with the Privacy concept should necessarily be built as a boundary object<sup>1</sup> benefiting to all project partners. In this respect, it aims to give a focused review of the privacy dimensions for the following reasons:

---

<sup>1</sup> « Boundary objects are both adaptable to different viewpoints and robust enough to maintain identity across them.” [1] Griesemer, J. and S. Star, *Institutional Ecology*, Emmanuel Anjembe – « La composition de fictions axiomatiques au service de la recherche technologique » - Thèse Grenoble Universités – 2013



- First, the concept being strongly rooted in the common sense, privacy has thus manifold definitions. Hence, the social scientist needs to deconstruct these definitions to work on privacy as a valid object of social research. Despite this social research process is common to social sciences, defining privacy remains a subject of interdisciplinary disputes when this does not fuel row within a common disciplinary field.
- Second, our purpose is to make our study **a helpful resource for the design of one precise technological device, the CPM Manager**. For this reason, this state of the art's structure is built as an insight into privacy, as a social concept being technologically understandable and of course, translatable.
- Third, in link with the two first reasons, a sociotechnical stance<sup>1</sup> is adopted throughout this section. This means that a set of different scientific traditions is used to understand the privacy issue in the design of a technological device. Consequently, we have tried to locate this section at middle stage between the bottom up approach (focused on human factors) and the top down one (focused on security technologies) [2]. This being said, the knurled bonds that tightly links privacy with technology, to be disentangled, need to be put in an introductory context.

Information and communication technologies (ICT) have swelled massively throughout the twentieth century. Along with other concerns, their use and diffusion have raised numerous questions about the ability of democratic states to prevent these technologies from threatening some of its values and interests. As a core value of the western societies' social order, privacy is claimed to be jeopardized by the implementation of such innovations. Therefore, the protection of privacy demands our societies to set different plans at several levels to take up this major challenge. Though, before the threat to be fought, the concept needs to be clearly defined to know what exactly is at stake. In the first part of this section (called *concept brief historical account of privacy*), we will cast an overview on the different ways the concept can be thought, depending on the specialist point of view. Further down this report, we will then adopt a the sociotechnical standpoint (called *Designing for Privacy: a sociotechnical standpoint*), in order to highlight what can be at stake when emerging technologies are righteously taken into account in the relations that question privacy today.

---

*Translations and Boundary Objects: Amateurs and Professionals in Berkeley's Museum of Vertebrate Zoology (1907-1939)*. Social Studies of Sciences, 1989. 19.

<sup>1</sup> See the further section called *Designing for Privacy: a sociotechnical standpoint*.

- ***A brief historical account of privacy***
- **The individual's birth and the dawn of a concept**

Now largely used in the common language, the concept of privacy burgeoned during the eighteenth century. It is strongly linked to the emerging consciousness of the individual. As Pierre Demeulenaere states: “*Le droit à la vie privée s’inscrira dans la continuité d’une telle revendication de droits individuels (conçus ou non comme naturels). Pour parler d’un droit à la vie privée, il faut déjà que l’on se situe dans une société où la notion de droits individuels s’est affirmée.*” [3]. Thus, the notion of privacy is profoundly rooted in the classical theory of human rights and individual freedom and individual property<sup>1</sup>.

François de Singly [4] has for instance noted the displacement of the concept from the thirteenth century to the twentieth century regarding family: the thirteenth century is characterized by the beginning of a long scale movement establishing the family as a social cell as opposed to the state. This movement took then a particular shape during the nineteenth century, when habitations were materialized as forms of reduced nuclear family cells – parents and children. During the twentieth century, the individual is confirmed as a new legitimate cell in opposition of the family itself.

This long and winding road of privacy<sup>2</sup> seems to reach its epitome with the appearance of the concept in international law texts in the aftermath of World War II. The Universal Declaration of Human Rights stands as a sound acknowledgement of privacy as a concept necessarily related to that of the individual. Article 12 states: “*No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honor or reputation. Everyone has the right to the protection of the law against such interferences or attacks.*”

The European Convention on Human Rights, Article 8, states: “*Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no*

---

<sup>1</sup> Cf. Locke J. ((1681)) (1993) *The Second Treatise of Government: An Essay Concerning the True Original, Extent, and End of Civil Government*, Penguin Books; J.S.Mill (1990) *De la liberté*, Gallimard, Folio; Moore B. Jr, *Privacy: Studies in Social and Cultural History*, New York, M.E.Sharpe, 1984; Rousseau JJ. ((1762)) (1943) *Du contrat social*, Paris, Aubier Montaigne ; Tocqueville A de ((1840)) (1986) Paris, Robert Laffont, collection « Bouquins ».

<sup>2</sup> We can see [5] Ariès, P. and G. Duby, eds. *Histoire de la vie privée*. 1999, Points: Paris. if we want a comprehensive account of privacy, in a historical perspective.

*interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”*

These two examples are institutionalized forms of what Bennett and Raab call the “privacy paradigm”, that is a set of assumptions based on more fundamental political ideas: *“The modern claim to privacy ... is based on a notion of boundary between the individual and other individuals, and between the individual and the state. It rests on notions of a distinction between public and private. It rests on the pervasive assumption of a civil society comprised of relatively autonomous individuals who need a modicum of privacy in order to be able to fulfil the various roles of the citizen in a liberal democratic state.”* [6].

Understanding privacy as a paradigm born from the historical establishment of a set of political ideas – liberal democratic societies – gives us clues to take into account the underlying contingency of the concept. On the one hand, it already gives it the qualities of a cultural and historically constructed concept. The emergence of the individual as an entity endowed with inalienable rights is a movement peculiar to western advanced societies. As a result, the social use of privacy should be handled with care when addressing it in a *non* western community. Its accepted meaning could be different or not taken for granted. On the other hand, it enables us to understand the normative power of privacy: the individual, human rights, democracy, all belongs to these undisputed latent concepts’ family that lies behind privacy in western societies. As a result, and as for any human rights or fundamental law, privacy is a concept of such value that it demands specific defence mechanisms.

This brief account of the expansion of the privacy concept allows us to value its particular strength in our societies. Nevertheless, the spread of information technologies at the beginning of the 1960s has initiated a period of thoughtful consideration of the privacy issue that profoundly reshaped the concept.

▪ **Information privacy<sup>1</sup>, a concept that bolsters Privacy definition**

The spread of information technologies within the agencies of the democratic states has posed a number of interrelated problems and challenged a variety of values and interests. In the 1960s and 1970s, the most immediate issue that captured the attention of policymakers was embraced by the vague and all-encompassing terms of information privacy or data protection. Indeed, in being rethought in regards to these strong innovative upheavals, privacy had been subjected to important changes in its definition.

On the one hand, we can consider that the inclusion of information processing as a particular dimension of privacy issue gave rise to a more dynamic meaning of the concept wherein the individual still plays a pivotal role [8]. This turn is particularly obvious when we examine two definitions of privacy that almost systematically appear in any information technology related work that considers privacy as a major concern. Those are Arthur Miller's: "*giving individuals the ability to control the circulation of information*" [9] and Alan Westin's: "*[privacy] meant the claim of individuals to determine for themselves when, how and to what extent information about them is communicated to others*" [10].

On the other hand, we can think with Bennett of this informational turning point as the result of both the hopeless attempt of building an all encompassing definition of privacy and the desegregation of this concept [11]. By asserting it, we do not want to say that information privacy wholly replaced an "*out-of-date*" definition of the concept. Somewhat information privacy is an additional under-layer of the wide-ranging privacy concept that has been added thanks to the fast growing technological change and its institutional recognition by our societies.

These two major evolutions were evenly followed by institutions. This turning point has been institutionally acknowledged by being integrated in the legal architecture of western countries. Historically, the first data protection law of world was stated by the German state of Hessen in 1970 followed by Sweden in 1973. As we have seen earlier, the cultural contingency of the definition of privacy is expressed through the type of protection states

---

<sup>1</sup> "*Information privacy meant that personal data could only be provided to a public or private organization for the purpose of fulfilling a legitimate social task*" [7] Bennett, C.J., *Computers, Personal Data, and Theories of Technology: Comparative Approaches to Privacy Protection in the 1990s*. Science, Technology, & Human Values, 1991. 16(1): p. 51-69.

have adopted. For example, the United States of America's way of legislating it is often opposed to the European law tradition – in particular laws and rules of European Community (now, European Union). On the other side of the Atlantic, sector-specific laws are adopted in respect to the atavist self regulation philosophy that inspires the legislator. Moreover, this sectorial case-by-case approach is privileged. In Europe, strong privacy laws sets are preferred; no differences are made in their enforcement between the states and the industry actors. Besides, a large number of privacy commissions have been set up as watchdogs. At the EU level, this was converted into the 1995 Data Protection Directive 95/46/EC which sets a benchmark for national law for processing personal information in electronic and manual files. This law act followed the 1980 OECD fair information practices which is a Voluntary Guidelines for Members to Ease International flow of information.

individu

All these alternative legislations<sup>1</sup> are, as Syrey observed, attempts to regulate a market navigating between personal data - e.g. information privacy -marketing and privacy protection business [12]. This necessity of controlling these emerging markets was reinforced with late technological evolutions.

Indeed, this dynamic informational side of privacy has thrived along with the insertion of new information technologies in everyday life. Information privacy has seemed to go through a new stage in the progression of its definition since the 1990s. Mark Weiser's now famous vision of third generation of computing<sup>2</sup> [13, 14], e.g. "*ubiquitous computing*"<sup>1</sup>, has

<sup>1</sup> For an overview of privacy-related laws in different countries, see <http://www.privacyinternational.org/>

<sup>2</sup> The first generation was characterized by large mainframe computers in the 1960s and 1970s. The second generation distinguishes itself by the introduction of standalone desktop computer (Personal Computer- PC) into homes in the 1980s and 1990s.

fostered the reduction of the scope through which privacy was being reasoned. Bohn *et al.*'s wording of the issue is particularly eloquent: "...these emerging technologies have forced us to ask a very important question: What are the implications of these [technological] challenges for the meanings that we, as a society, want to assign to personal privacy and for the legal protections that we want to give to it?" [15].

This next generation computing environment would be one "*in which each person is continually interacting with hundreds of nearby wirelessly connected computers*" [14]. With ubiquitous computing, the traditional reasons which until then justified privacy protection measures became insufficient in regards to the set of generic privacy concerns that ubiquitous networks will very likely raise for users according to Mark Ackerman [16]: "*A pervasive network of interconnected devices and communications will mean that the sheer quantity of personal information in circulation will increase greatly; the introduction of perceptual and biometric interfaces for certain applications, will transform the qualitative nature of personal information in circulation; in order to personalized services, ubiquitous networks will require the tracking and collection of significant portions of users' everyday activities*". Hence, legal scholar Lawrence Lessig identified four arguments that encompass all the dimensions of the concept and extended the initial privacy paradigm [6]. **Privacy is then understood as:**

- **Empowerment for people to control information:** Here, privacy is mainly understood as informational privacy. Apart from what has been stated earlier, we can add that the status of personal information is what is at stake here: should it be seen as private property or as intellectual property?
- **Utility:** Privacy matches here Warren and Brandeis' reductionist definition of it, "*The right to be left alone*" [17]. Privacy is thus a utility that protects the individual against any kind of nuisances.

---

<sup>1</sup> "*Ubiquitous Computing (UbiComp) and/or Ambient Intelligence (Aml) refer to a vision of the future information society where humans will be surrounded by intelligent interfaces supported by computing and networking technology that is everywhere, embedded in everyday objects such as furniture, clothes, vehicles, roads and smart materials. It is a vision where computing capabilities are connected, everywhere, always on, enabling people and devices to interact with each other and with the environment. Computer devices are becoming increasingly small and cheap, interconnected and easy to use in order for them to find application in all aspects of our everyday lives. Computing capabilities will therefore not only be available in computing devices but also in everyday objects. These devices will be able to sense, think and communicate.*" as in Punie, Yves. (2003). *A social and technological view of Ambient Intelligence in Everyday Life* (Technical Report EUR 20975 EN): Institute for Prospective Technological Studies, Directorate General Joint Research Centre, European Commission.

- **Dignity:** The dignity is secured by the reciprocal obligations between parties involved. This dimension here lies on the necessary balance between the loads of information people are exchanging.
- **Regulating agent:** Laws and moral norms addressing privacy are tools that ensure the administration of corporate organizations cannot take advantage from their position. It limits their ability of information gathering and of surveillance.

This expansion of the domains that privacy covers – which in parallel implies a substantial enlargement of the domain of privacy protection – forces us to acknowledge the relative instability of this concept. We have demonstrated that **privacy is a historically constructed concept whose growing societal weight could notably be observed by focusing on its embodiment in law norms**. Hence, drawing on Lessig's work enables us to highlight the very contingency of this concept. The numerous dimensions of privacy can be explained by the relative discrepancy that the concept experiences in its treatment depending on which institution uses it.

- ***The very contingency of a concept***
- **Finding common points in contingency**

Until now, we have essentially tackled the privacy issue through the lens of law and political philosophy. However, it would be misguided to assert that in doing so, we have an adequate guidance of what counts today as privacy [18]. In this respect, Lessig's reflection of privacy incentives fosters us to explore the contingency of the concept when confronted to different social sciences' backgrounds. We will see that despite this contingency, invariant characteristics of privacy can be highlighted.

Sociologically, despite a large array of different definitions, privacy is consensually thought to be a strongly contingent notion. Not only that it is equivocal when used in the common sense, but also sociologists particularly insist on the scientific relativity of the concept. Hence, Demeulanaere asks: "*Qu'est-ce qui relève exactement de la vie privée ? La difficulté tient à ce que la notion de vie privée est relative, les mêmes actions pouvant quelquefois d'un certain point de vue apparaître comme privées ou au contraire comme publiques à partir d'une autre perspective également acceptable.*" For instance, the definition of privacy is dependent of one's position on the socioeconomic ladder [19], on different context and roles [20], and so forth.

This inherent subjectivity of what comes under privacy is observed by any social scientist. The second important point lies in the significance given to the context. Following –

but non comprehensive – examples are showed as an illustration of the multiples variants of this shared assumption:

Sociologist scholar Bates' definition is that of *"a person's feeling that others should be excluded from something which is of concern to him, and also a recognition that others have a right to do this. It is assumed that this recognition of another's right to privacy is widely shared in a population and given rather specific form in the culture"* [21]. This definition is then centred on the individual perception of privacy that is socially constructed and context-related. The rules of the interaction<sup>1</sup> are the bottom line of what privacy means for a social group. The author defines three specific ways around which privacy is structured:

- The **differentiation into many content areas**: The author, here, distinguishes between things related to the self that cannot be negotiated and things related to different selves that can be differently perceived.
- Secondly, privacy is **structured by the answer a person gives to the question**, *"Who are the persons you wish to exclude from having this knowledge?"*
- Thirdly, **privacy is structured by situational contexts**.

With a socio-psychological point of view, Schwartz insists on the links that bond privacy and personal property [24]. Hence, he differentiates two types of objects, whether they are body or non-body objects: those which may be observed by the public (and which may be termed personal objects) and those which are not available to public view (private property). The latter one is defined in terms of *"those intimate others who may have access to it in terms of visibility of use. Some private objectifications of self may be observed by family members, but some may be observed by no one except the self. There is no doubt that these latter objects have a very special meaning to identity; some of these are sacred and must not be contaminated by exposing them to observation by others; some are profane and exposure will produce shame, but both are special and represent an essential aspect of self and, from the possessor's point of view, must not be tampered with."* **Here, the different status of the objects shall be only understood in regards to their owner and its environment. Hence,**

---

<sup>1</sup> Not only between classical social actors... If we extrapolate, we can consider humans and non-humans to be of same importance. See for example [22] Latour, B., *Where Are the Missing Masses? The Sociology of a Few Mundane Artifacts*, in *Shaping Technology/Building Society*, W. Bijker and J. Law, Editors. 1992, The MIT Press: Cambridge London. p. 226-258 & [23] Latour, B., *Science in Action. How to follow scientists and engineers through society*. 1987, Cambridge: Harvard University Press.



**characterizing the property not only means defining the access to it or valuing it.** This extremely relativist – constructionist, would say the sociologist – standpoint advocates for considering what people claim to be personal privacy. In that way, intrusion could not be reduced to what the law considers to be intrusive.

Evenly, thinking of the law to be an unambiguous tool to address privacy becomes daunting when considering the legal force with the eye of political science, and particularly public policy. Data protection laws were enacted as a policy response to the privacy problem among advanced democratic state. In this respect, Bennett [11] **distinguishes three different ways to regulate information technologies in order to protect personal data and to enhance personal privacy:**

- **Institutional accountability theory:** Privacy is here an issue that is used as a conceptual means, amongst others, to counterbalance the power of institutions. For this theory, any kind of institutionalized institution power, e.g. any forms of state-related organization, corporate companies, and so forth, is strengthened by information technologies. As Stone and Warner [25] admonished: *"the computer has given bureaucracy the gift of omnipotence, by putting into its hands the power to know. No fact unrecorded, nothing forgotten or lost, nothing forgiven"*.
- **Civil rights theory:** this theory is focused on the individual. Drawing on classical liberal doctrine, it advocates for the sovereignty of the individual above all.
- **The technology control theory:** this approach could be said to belong to technological determinist views in the way that it relegate humans to marginal decision-making. Here, technologies are understood to mould social relations. Hence, public policies play a minor role in comparison to the importance attached to technologies. As Priscilla Reagan says: *"This technological approach is not concerned with the relationship of the individual and his personal information, nor with the individual and the bureaucracy. Rather it concentrates on the computer and information, and the computer and the bureaucracy's information handling"* [26]. Privacy is then primarily tackled in technological terms, as a problem to ensure through technological safeguard that *"right people use the right data for the right purposes"* [27]. Privacy protection is then oriented toward the design of technical devices that intervene throughout the information process. James Katz underlines the strong correlation bonding privacy-protecting technologies development as a response to privacy-invading technologies [28].

By focusing on institutional actors, public policy tackles the privacy issue by considering information technology in regards to the organization-individual relationship. Hence, the manipulation, storage, collection or disclosure of personal data is at the heart of the debate. Fears are rooted in the belief that organizations accountability, human dignity, individuality could be compromised by the spread use of information technologies. It is in this

disciplinary field that the concept of surveillance is paramount<sup>1</sup>. In addition, despite the fact that these three different public policies philosophies can be intertwined, we have chosen a more thoroughly description of the technological control theory as it largely inspires the ambition of protecting privacy through design<sup>2</sup>.

In this part, we have illustrated by a few examples how contingent the concept of privacy was when addressed by different disciplinary fields. However, though scholars stress different aspects of it depending on their discipline centres of interest, invariants can be found amongst those analyses. **Privacy is seen as being necessarily prone to the subjectivity filtering of the involved actors, their interpretation of it being strongly dependant of the context within which interaction occurs. Moreover, these analyses underscore the fact that privacy establishes an *in* and an *out* difference between what can be disclosed or not; between what group is authorized or not to access this information. In this way, they prove privacy to be a concept that discriminates.**

▪ **The border paradigm: underlying the dynamic side of privacy contingency**

Demeulanaere [29] establishes though a very sharp distinction between two different variables to consider when trying defining privacy. He first highlights the ability of an individual to control any action in interaction. He then talks about secrecy as another process that enables the individual to keep some information, some actions undisclosed. The concept is broke down by the author who distinguishes then three different incentives to keep something “*out of the public glance*”:

- Secret as a recognized social norm (activities that take place in the toilets).
- Secret as a means to perform illegal activities (heroin consumption).
- Secret as a means to protect one’s personal interest (hiding presents before Christmas).

Demeulanaere, in insisting that privacy has no unique counterpart – what is secret can be public and vice versa – appends complexity to this discrimination process. Borders defined

---

<sup>1</sup> “*Surveillance*” is also related to privacy, but implies something quite specific as the intentional observation of someone’s actions or the intentional gathering of personal information in order to observe actions taken in the past or future. Unwanted surveillance is usually taken to be an invasion of privacy. This concept highlights the importance of privacy as a utility that protects people against unwanted intrusions and the right to be left alone.

<sup>2</sup> See next section (*Designing for Privacy*).

by privacy are numerous, as sociologist scholar Gary T. Marx proves, when considered in a subjectivist way.

Marx, drawing from the perceived privacy violation, tackles this issue by looking at this discriminating act as a process of *border crossings* between the public and the private, what he calls “*murky conceptual waters*” [30]. Border crossings are “*Central to our acceptance or sense of outrage with respect to surveillance... are the implications for crossing personal borders.*” He defines four kinds of border crossings:

- **Natural borders:** Physical limitations of observations, such as walls and doors, clothing, darkness, but also sealed letters, telephone calls. Even facial expressions can form a natural border against the true feelings of a person.
- **Social borders:** Expectations about confidentiality for members of certain social roles, such as family members, doctors or lawyers. This also includes expectations that your colleagues will not read personal fax messages addressed to you, or material that you left lying around the photocopy machine.
- **Spatial or temporal borders:** The usual expectations of people that parts of their life, both in time and social space, can remain separated from each other. This would include a wild student time that should not interfere with today’s life as a father of four, or different social groups, such as your work colleagues and lovers in your favourite bar.
- **Borders due to ephemeral or transitory effects:** This describes what is best known as a “fleeting moment,” an unreflected utterance or action that we hope gets forgotten soon, or old pictures and letters that we put out in our trash. Seeing audio or video recordings of such events later, or observing someone sifting through our trash, will violate our expectations of being able to have information simply pass away unnoticed or forgotten.

This brief overview of privacy history has enabled us to see how normative this concept was after all. Because it is strongly rooted in western liberal philosophy and has been acknowledged to be so important to advanced democracies that it requires adequate norms to be protected. However, this unquestionable side of the concept has fostered stunning reactions in these early stages of an era that some calls the *transparent society* [31], a society wherein privacy would be condemned to be an obsolete term. This clear-cut vision of the future, though marginal, is not the only one: Scott McNealy’s famous “*You have no privacy anyway, get over it*” [32] and Peter Cochrane’s “*All this secrecy is making life harder, more expensive, dangerous and less serendipitous*” [33] indicate a growing backlash among those tired of hearing the constant warnings coming from privacy advocates. Those who acknowledge the

contingency of the concept could then adopt a sociotechnical standpoint that evacuates the reductionist translation of privacy in security problems only. This is what we are going to see in the section devoted to the sociotechnical aspects (called *Designing for Privacy*).

## ■ Privacy and RFID (CEA)

### ■ *Introduction of contactless systems*

The contactless systems addressed in this paper are based on communication of radiofrequency type and consist of a reader emitting an electromagnetic field and a passive contactless object collecting its energy from the electromagnetic field. This latter is also used to transfer data in both directions. These contactless systems are characterized by a trade-off between range and complexity. Basically the field emitted by the reader decreases with distance, thus the further away the portable object, the lower the power supply and the smaller the power of computation of the embedded processing.

For example, RFID identification tags will give priority to operating distance: from a few centimeters to a few meters to the detriment of embedded computing or processing functions. In this case, exchanges will have minimum confidentiality, the data flow between the reader and the tag will be relatively small and the data processing carried out on the tag will be very simple, if any. On the other hand, remote reading of the tag without awareness of the owner will be particularly easy when tag range is large and its processing capabilities minimum.

However, smart cards, suitable for the handling of more confidential data, will give priority to computation and processing in order to perform complex security tasks such as: cryptography calculation to authenticate the holder and protect data, secure storage of sensitive information in non volatile memory, use of more efficient operating system for multi-application management and downloading of new service applications. These contactless objects, on which a microcontroller is embedded, will have to collect more energy from the electromagnetic field emitted by the reader and thus operate in near field. In this case, exchanges with a very high degree of confidentiality and a higher data rate will be mandatory. However, due to operation in near field, the holder of the contactless object will have to make a voluntary gesture for the transaction to take place a few centimeters from the reader. Conversely, readers will have to be a few centimeters from the object to run a transaction.

To enable worldwide interoperability of a contactless system, ISO international standards have been published: the family of ISO 18000-x standards for RFID identification tags covering the frequencies bands of 125 kHz, 13.56 MHz, 433 MHz, UHF(868-915MHz), 2.45 GHz and the ISO 14443-x standards for contactless proximity cards at 13.56 MHz and ISO 15693-x standards for contactless vicinity cards, also at 13.56 MHz. These standards describe the air interface part of the communication channel and thus allow any reader to decode information transmitted by a contactless object and vice versa. To decode doesn't mean to decipher, of course, and covert transaction are possible and manageable at transport or application layers. To ensure reliability of exchanges and prevent interpretation of content, data can be encrypted by means of a secret shared by the card and the reader.

Standard ISO 14443 also describes frame formats and collision management: a deterministic approach for type A and a probabilistic approach for type B, associated with the communication protocol and specific commands for contactless cards.

### ■ *Comparing contactless cards with contact cards*

Three main differences can be pointed out:

Comparing contactless cards with contact cards, three main differences can be pointed out:

- The use of a RF channel
- The remote power transmission
- The multi card identification protocol

- RF Channel: The use of a RF channel whatever the operational range or standard enables new possibilities of spying the communication over the air between the reader and the card. Because there is no physical contact, the reader and the card do not know which distance they are separated from. They are only aware that, anywhere in a presumed close volume, “something” is trying to exchange messages with them, hopefully with the right protocol. Furthermore they have no basic means to detect a third party in the operation volume. Because of the rapidly decreasing HF electromagnetic near field, received signals may present a huge dynamical range, the well known near/far problem. Relative movements may mask or unmask cards or devices.

- Remote power transmission: Basically the contactless card is remotely supplied through the harmonic electromagnetic field. It is important to point out that this function allows anybody or anything with an appropriate device to start a transaction with a passive card without the awareness of the owner of the card. However, near field communications such as ISO 14 443 standard, enables basically short operational distances (i.e.: < 10cm), thus reducing long distance possibilities for power supplying. For very simple contactless devices, the harmonic field provides also the clock. In that situation, the reader/card couple is a synchronous one, preventing clock shift that decrease efficiency of wireless modems.

- Multicard protocol: Because several cards can be together in the electromagnetic field of the reader, the protocol has to manage a specific initial phase of the protocol in order to inventory the full set of cards that are present in the field. This is the so-called singulation phase which is performed before the authentication phase. So far and of course in this singulation phase, there is no ciphering of the exchanged messages. Messages are in clear text according to ISO 14 443-3 standard. Only the identification parameter (UID) of the card can be a random one, providing some anonymity.

#### ■ ***Economical and Societal context and trusted computing***

The main debate on RFID at the societal level is security versus privacy. Many companies that deploy contactless systems are profit companies and fraud is a severe

competitor. Security is basically promoted by operators for evident reason of preventing economical losses or unauthorized accesses to subscription-based services. In some commercial or economical aspects it is also mandatory to protect the users. The targeted asset of attacks is the business. Fraudulent attacks on the contactless technology have to be nullified.

Privacy is only a matter of concerns for users that will live more and more in a digital world with one or several digital doubles. Here the asset is individual freedoms and more specifically in this case the protection of digital personal data.

With the trumpeted arrival of Ambient Intelligence, digital data privacy is a key point. Several contactless low resources smart devices have shown some connections with privacy concerns:

- RFID electronic tags for items identification in supply chain at retail stores.
- e-Citizen contactless cards (e-passport, e-identity, ...) for person identification

For the daily usage of this emerging and rapidly spreading technology, some questions arise from the basic user, such as:

- Do I communicate with the right reader?
- Is somebody spying my transaction?
- Is somebody trying to communicate with my passive device?
- What are the data exchanged over the air?

Here, it should be pointed out that not only the users but operators that deploy the system ask for quite the same questions. The former want to protect his privacy, the latter to protect his business. In both case they need to trust the trusted computing supported by these contactless portable objects and must understand the underlying security in order to trust it.

RFID electronic tags: The concept of ambient intelligence (or AmI) is a vision where humans are surrounded by computing and networking technology unobtrusively embedded in their surroundings. The privacy concerns have been raised very early with the introduction of

RFID smart devices. In particular the introduction and potential generalization of electronic tags on mass markets products and at the retails level at every shop or supermarket have enlarged the potentiality of traceability of persons. The interoperability of automatic data capture systems and the combination of tagged items carried by a person may be used to trace and to locate this person when moving in commercial centre or urban areas.

e-Citizen contactless cards: Concerns are also very high with the use of contactless e-passport. Some hostile distant reader may check your nationality and trigger attacks. A same scheme may be ruled out with an identity card. High sensitive privacy personal data may be potentially downloaded from contactless health cards without the agreement of the owner.

Among the basic fears that users, consumers and citizens raise when addressing the contactless technology, one can mention:

- 1) A human person cannot sense the electromagnetic field
- 2) The identification code is unique. Comparing with the bar code, the RFID code includes the serial number of the items that enables total traceability. Groups of electronic identifiers (RFID) turn out to be a signature of a person and so to be traced easily.
- 3) RFID readers are small enough to be embedded in a cell phone.
- 4) The localization of person is possible when she is close to a reader
- 5) Citizens and consumers do not have access to the history of the readings.

In that “privacy situation”, the main drawback of these contactless systems is that there is no switch on/switch off mechanism to assess the will of the owner to use them. They can be remotely and covertly activated and triggered without the awareness of the owner. So trust starts to shift down.

Privacy is the ability of an individual or group to keep their lives and personal affairs out of public view, or to control the flow of information about him. It is clear that AmI may endanger the privacy of citizens. On the other hand, AmI aims to offer a lot of on-line services that anybody can get only if he identifies himself or the items he is dealing with. So is the difficulty.

## ■ *Security models for contactless cryptographic protocols*

We describe here specific cryptographic protocols that have already been designed in order to create a secure channel between a contactless device and a terminal.

This kind of protocols – usually called “password-based key establishment protocols” are defined in the following context:

- a chip with sensitive contents  $\sigma$
- a terminal (or server) with no cryptographic material
- a low-entropy password  $\pi$ 
  - known by the chip
  - given to the terminal at transaction time
- the chip wants to send  $\sigma$  securely to the terminal

In a classical approach, for each considered protocol, we aim at giving cryptographic security arguments telling

- Which security requirements are fulfilled: using a security proof
- Which are not: by showing an attack

A security notion directly reflects a threat. To define precisely a security notion, we have to specify

- An adversarial goal: what is the attacker trying to do ?
- An attack model: what has the attacker access to ?

There are several security notions, each of which reflects a specific attack scenario.

In the context defined above (a contactless chip and a terminal), the usual security notions are the following:

- Basic security notions
  - Secrecy = passive/active authentication does not reveal  $\sigma$
  - Forward secrecy = passive/active interaction does not reveal  $\sigma$  even if  $\pi$  known
  - Password privacy = resistance to offline dictionary attacks on  $\pi$
- More subtle security notions
  - Untraceability = cannot trace chip identity afterwards
  - Unlinkability = traces are unlinkable



- Non-transferability = terminal cannot prove transaction to third parties

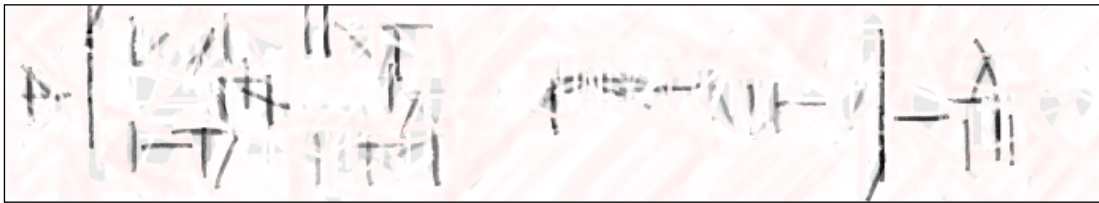
To describe these security notions more formally, we will use the following notations:

- Protocol traces
  - $T(\pi; \sigma)$  distribution of a random co-execution with  $\text{chip}(\pi; \sigma; \cdot)$
  - $T \leftarrow T(\pi; \sigma)$  a random protocol trace
- Logical access to chip
  - $\text{chip}(\pi; \sigma; \cdot)$  : oracle access to  $\text{chip}(\pi; \sigma; \cdot)$
  - $\text{Achip}(\pi; \sigma; \cdot)$  : attacker A plays around with  $\text{chip}(\pi; \sigma; \cdot)$

## 1. Secrecy

The intuition of this security notion is the following: it should be hard to recover  $\sigma$  without knowing  $\pi$  even with logical access to  $\text{chip}(\pi; \sigma; \cdot)$ .

Formally, an attacker A is said to  $(\epsilon; \tau)$ -break  $(n; k)$ -Sec if A runs in overall time  $\tau$  and

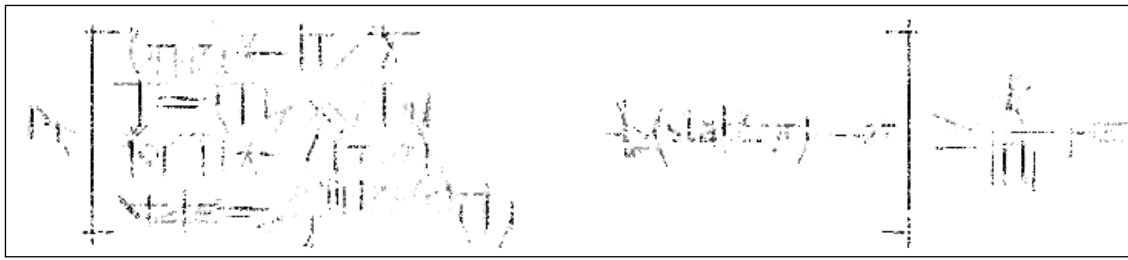


where A can engage in up to  $k$  protocol executions with  $\text{chip}(\pi; \sigma; \cdot)$ .

## 2. Forward secrecy

The intuition of this security notion is the following: protocols executed in the past should remain secure even though the password  $\pi$  is revealed to the attacker

Formally, if we denote  $A = (A_1; A_2)$  (play stage and open stage),  $A = (A_1; A_2)$  is said to  $(\epsilon; \tau)$ -break  $(n; k)$ -ForSec if A runs in overall time  $\tau$  and



where  $A_1$  can engage in up to  $k$  protocol executions with  $\text{chip}(\pi ; \sigma ; \cdot)$ .

### 3. Password privacy

The intuition of this security notion is the following: An online protocol run should rule out only one guess on  $\pi$  (= resistance to offline dictionary attacks on  $\pi$ ).

Formally,  $A$  is said to  $(\epsilon; \tau)$ -break  $(n; k)$ -PwdPriv if  $A$  runs in overall time  $\tau$  and



where  $A$  can engage in up to  $k$  protocol executions with  $\text{chip}(\pi ; \sigma ; \cdot)$ .

A refinement of this notion is called  $(n; k)$ -PwdPriv $^+$  :  $A$  is also given  $\sigma$ .

### 4. Untraceability

The intuition of this security notion is the following: there should be no way to tell whether protocol traces relate to a given chip. This captures a strong form of privacy.

Formally, we say that  $A$   $(\epsilon; \tau)$ -break  $n$ -UnTrace if  $A$  runs in runs in overall time  $\tau$  and



## 5. Unlinkability

The intuition of this security notion is the following: telling apart which ones relate to the same chip and which do not should be hard to achieve.

Formally, we say that  $A$   $(\epsilon; \tau)$ -break  $(n_1; n_2)$ -UnLink if  $A$  runs in runs in overall time  $\tau$  and



## 6. Non transferability

The intuition of this security notion is the following: the terminal cannot prove transaction to third parties.

This notion is closely related to the concept of zero-knowledge in cryptography.

- ***Objects concerned: tags, contactless cards, NFC phone***

Three different kinds of object are concerned with RFID.

- **RFID tags**

The term RFID (Radio Frequency Identification) is normally devoted to electronic tags. The aim of those tags is to identify objects like an item in a supermarket with a unique code for each item contrary to bar code that only enables an identification of a product. RFID tags can be read from a 1 m distance. Two standards define RFID tags: ISO 18000 with different parts dealing with the different available radio frequency bands and EPC Global that is now a part of the ISO 18000.

- **Contactless cards**

Contactless card emerged when a contactless interface remotely powered was given to the smart card. This category can be split into the vicinity cards with a 1 m reading distance that are devoted to the identification of people and that are described in the ISO 15693 standard and into the proximity cards with a 10 cm reading distance that are devoted to application like payment, transport ticketing or electronic passport and that are described in the ISO 14443 standard. Contactless cards are limited to the 13.56 MHz band.

- **NFC phone**

The contactless interface was then introduced in a mobile phone to prevent from the user to wear many cards. NFC was first described in the ECMA 340 and ECMA 352 standards before being introduced in the ISO 18092 standard.

- ***Low Resources Devices and Security Issues***

RFID contactless devices support some very basic characteristics that bound drastically the security protections:

- 1) Passive devices: portable contactless objects are basically passive device and so don't support any embedded energy source. A first consequence is that a power on/off switch is

useless and there nothing to do for the user to start a transaction when the device is in an electromagnetic field.

- 2) Low Power device: the supply power which can be collected by a contactless device is very low or even ultra low. Basically there are two main families: a) smart cards that use the near field for a magnetic coupling and can collect roughly some few tens of mW at some centimeters (2 to 10) and b) electronic tags that use UHF fields and propagation mode and backscattering and can collect some few tens of  $\mu$ W at long range (3 to 7 meters). The result is that the power budget is too drastic for the chip to support complex security functions and embedded protections, if any, are very limited. So far, basic electronic tags don't support any protection.
- 3) Low Resources devices: Because of low power supply budget and low cost chip constraints the embedded computational power is not so large on smart card chips and allows roughly, in the best cases, bloc ciphering such as DES, TDES, AES, RSA and ECC. Basic electronic tag chips for items traceability don't support any encryption processing.
- 4) Low Cost Devices: The area budget on the surface of the die is hardly limited due to cost constraint. Security functions must be cheap. But we can notice that Moore's law helps to increase security functions at least for the digital ones.
- 5) One Reader and Many Cards or Tags Identification protocol (Anti-collision): Contrary to contact card systems where there is only one card connected to the reader, several cards may be into the electromagnetic reader field and collisions of messages can occur if not prevented. To tackle this problem, the first phase of the protocol is to identify all the present cards and to select only one to perform the transaction, which is the so called singulation phase.

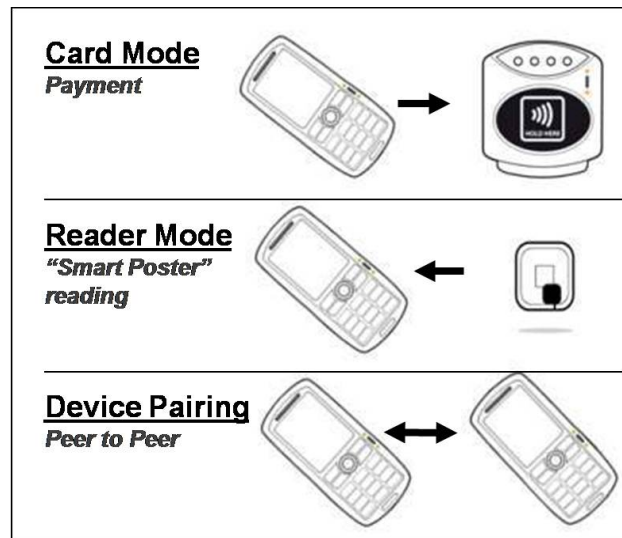
To conclude the low resources aspect of contactless devices, it is worth to mention that the reader enjoys in most case relatively large power supply and so can run high processing capabilities to manage digital receiver and cryptographic functions. We must to keep in mind that the contactless system is fundamentally an un-balanced one.

## ■ Introduction to NFC (INSIDE)

### ■ *Description of NFC*

NFC (Near Field Communication) is a RF (Radio Frequency) communication between electronic devices (mobile phones, PDAs, computers and terminals). It is derived from Contactless smart card technology. Operating at 13.56 MHz and transferring data at up to 424 Kbits/second, NFC provides intuitive and simple communication between electronic devices. The main characteristic of NFC is that it is a wireless communication interface with a working distance limited to about 10 cm.

Any NFC device can act as a reader and as a card.



**NFC various modes of use**

NFC technology is currently mainly aimed at being used with mobile phones. There are three main use cases for NFC:

- card emulation : the NFC device behaves like an existing Contactless card
- reader mode : the NFC device is active and read a passive RFID tag, for example for interactive advertising, or can discuss with a card
- P2P mode: two NFC devices are communicating together and exchanging information.

The underlying layers of NFC technology follow universally implemented ISO (ISO 18092), ECMA (ECMA 340), and ETSI standards.

### ▪ ***Brief History of NFC***

In 2000, Nokia wanted to have in its phone an interface which would allow a mobile phone to interact with some other objects simply by touching them.

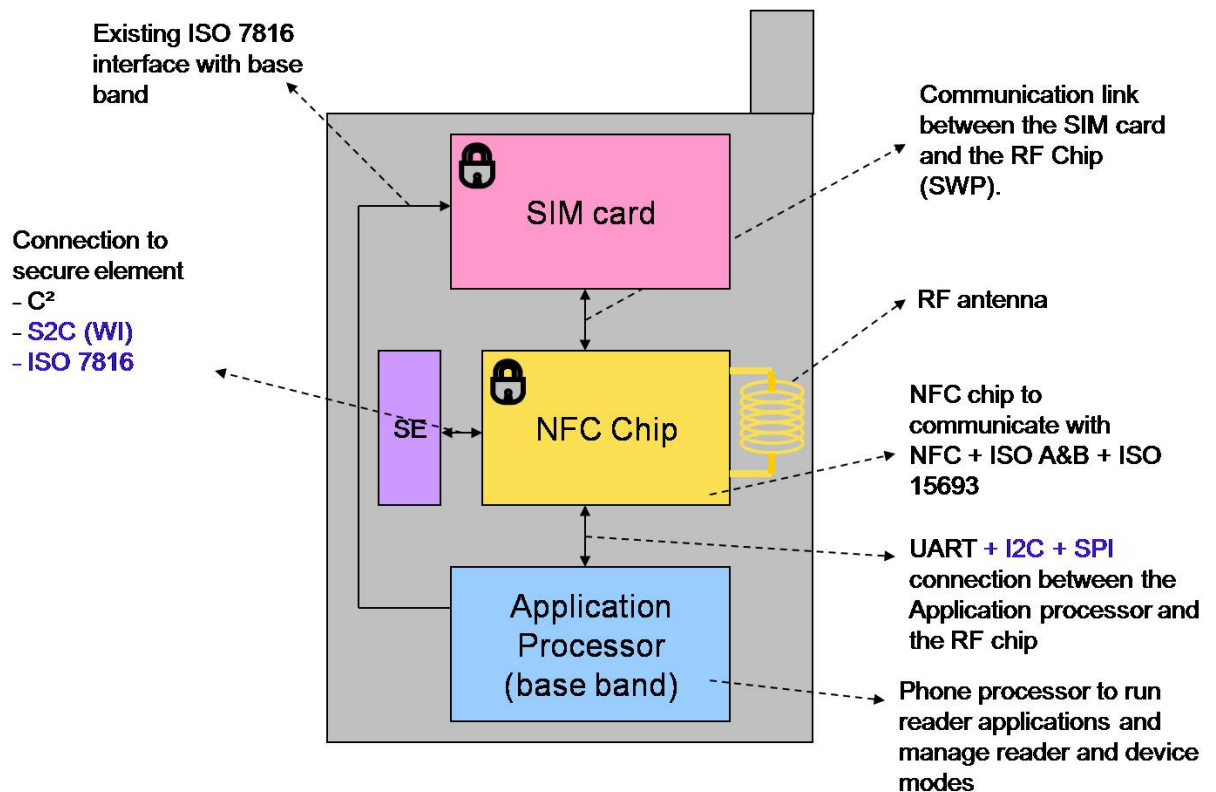
In 2004, NXP Semiconductors, Sony and Nokia founded the NFC Forum [NFC] to advance the use of Near Field Communication technology by developing standards-based specifications, ensuring interoperability among devices and services, and educating the market about NFC technology.

In 2006, the Forum formally outlined the architecture for NFC technology.

In 2008, the Forum has about 150 members and as of December, the Forum has released 11 specifications.

Although, NFC has been studied for 8 years, there is not yet any widely spread application for users. NFC is still under study and its deployment should really start and increase in the 2 incoming years.

### ▪ *NFC Mobile Phone Architecture*



#### **Support full architecture**

The Sim Card and the base band are the classic elements present in a mobile phone.

The NFC chip is then the new device which appears into the cell phone. It essentially acts today as a router and can be controlled either by the SIM or by the Base Band Processor.

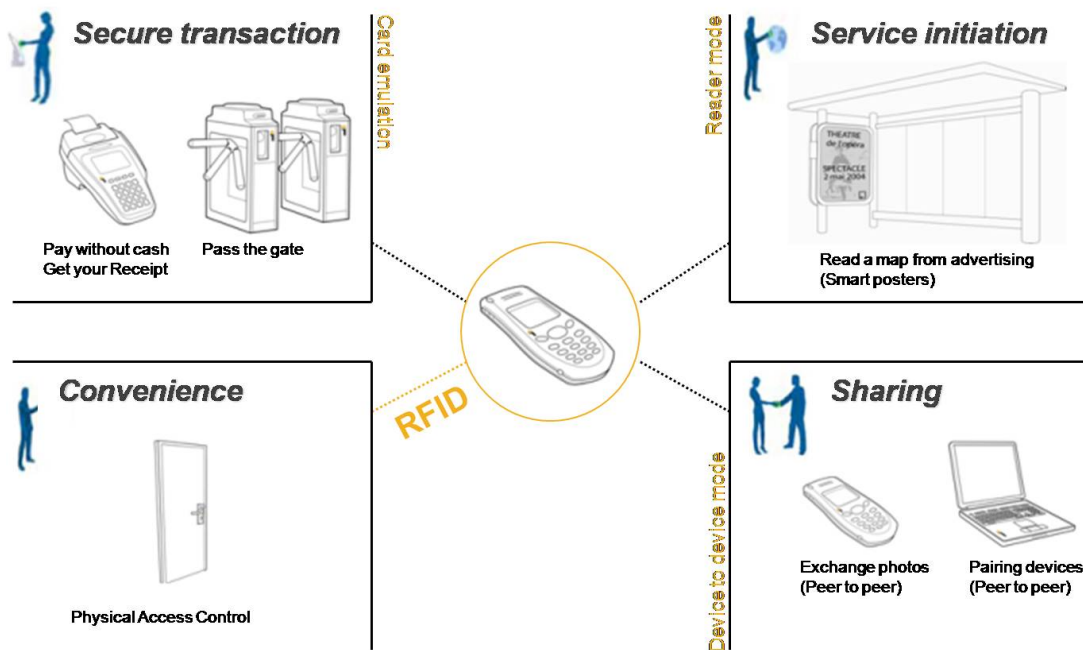
An additional card, named SE for Secure Element, can be also added. Its location isn't yet fixed. It may be the SIM or stacked on a NFC Chip or it can be another element as an additional chip or as a SD Card. It would be necessary to have a new chip if some secure applications which could not be added into the SIM card were necessary. In this case this SE is connected to the NFC.

This mobile phone with its NFC can be used in many applications [INS].

## ■ *Applications*

Plenty of applications are possible, such as:

- Mobile ticketing in public transport: an extension of the existing Contactless infrastructure.
- Mobile payment: the device acts as a debit/ credit payment card.
- Smart poster: the mobile phone is used to read RFID tags on outdoor billboards in order to get info on the move.
- Bluetooth pairing: in the future pairing of Bluetooth 2.1 devices with NFC support will be as easy as bringing them close together and accepting the pairing. The process of activating Bluetooth on both sides, searching, waiting, pairing and authorization will be replaced by a simple "touch" of the mobile phones.



**NFC various uses**

Other applications in the future could include:

- Electronic ticketing : airline tickets, concert/event tickets, and others
- Electronic money
- Travel cards



- Identity documents
- Mobile commerce
- Electronic keys: car keys, house/office keys, hotel room keys, etc.
- NFC can be used to configure and initiate other wireless network connections such as Bluetooth, Wi-Fi or Ultra-wideband.

## ■ Threats on NFC

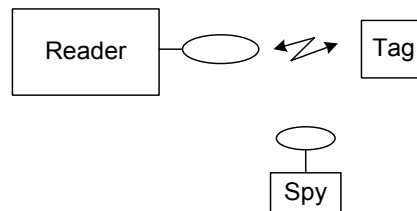
---

### ■ Current physical attacks on NFC-Systems

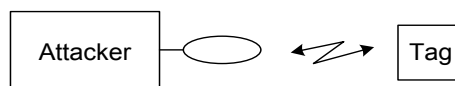
#### ■ *Eavesdropping*

Attacks on physical layer can be classified into two classes:

- Passive attacks which consist of **listening** on transactions between an authentic reader and an authentic contactless card. This attack is also called « eavesdropping ».



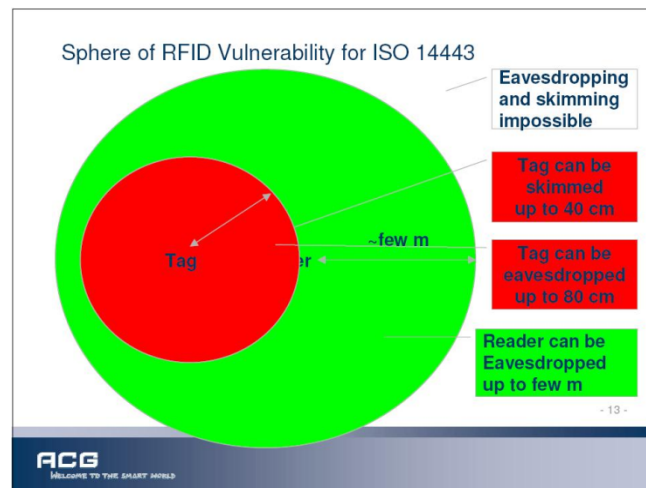
- Active attacks which consist of **reading** a contactless card. They include powering and modulation. These attacks are also called “skimming”.



First publications with practical results about eavesdropping mention the NIST<sup>1</sup> demonstration at the « National Biometric Security Project Facility » in 2004.

Using a reader equipped with a specific antenna, the NIST tester team was able to lift "an exact copy of digitally signed private data" from a contactless e-passport chip from 30 feet (9 m) away<sup>1</sup>.

<sup>1</sup> National Institute of Technology



Sphere of RFID Vulnerability [KR1]

No precision was given about experimental conditions and real performances. This lack of detail allowed a many different interpretations in different articles. It seems, in reality, that only uplink, i.e. reader-to-card communication has been intercepted.

In his talk in “Cartes 2005”, Peter KRONIGER distinguished the possibility to intercept information sent by the reader and information sent by the contactless card by taking in account the signal-to-noise ratio. He pointed out that the reader can be successfully listened to from a few meters while listening distance for contactless card is restricted to 80 cm, contradicting the NIST results. [KR1]

This distinction is also present in the BSI report, but with a larger (tens of meters) listening distance for the reader. Contactless listening distance remains restricted to about 5 times nominal distance given by manufacturer that is to say to about 1 m. [RI1]

---

<sup>1</sup> Neville Pattinson, director of business development technology and government affairs for smart-card provider Axalto Americas

T. Finke et H. Kelter (BSI) demonstrated through experimentations with a PEGODA reader (NXP) and a MIFARE card (NXP) that reader to card and card to reader communications can be intercepted up to 2 meters. [FIKE1]



*FINKE and KELTER experiment [FIKE1]*

Gerhard P. Hancke, University of Cambridge, provides details on means and methods (antennas, instrumentations, tunings...) to perform eavesdropping on a contactless transaction. [HA1].

Experiments with an AGC reader and ISO14443 A/B and ISO15693 cards were performed in his laboratory. According to his measurements, performances of different cards were

	ISO14443-A and ISO15693	ISO14 443-B
Reader to card	> 10 m	3 m
Card to reader	1 m	3 m



Experiment by G.HANCKE [HA1]

Distance activation is a much harder and more delicate problem to solve. First, we must be able to power the contactless card and then send commands by modulating the field.

### ▪ *Skimming*

Skimming entails two functions that are usually in conflict: we need an antenna with a high quality factor for generating a high magnetic field with minimum of dissipated power, however, at the same time, we need a large bandwidth and so a weaker quality coefficient for modulating the field and sending commands. These two operations can be made with separated devices equipped with distinct antennas but they must operate with the same clock.

As with passive listening, we must watch out for spectacular announces. For instance, a Flexilis team claimed at Defcon'05 to have set a new world record of passively reading a contactless card from 69 feet. In fact, they used an UHF chip and not a ISO-14443 device.

In the Kroninger study, energizing a contactless card at 50 cm distance is hardly feasible, however, energizing at 1 m is impossible, because dissipated power grows with the cube of distance. If we need only 0.5W for energizing a contactless card at a distance of 5 cm, we need 500 W at 50 cm, which is not easily achieved using portable power appliances. At 5 m, we would need 500 kW- thus, it would not only be a problem of portable power generation, but also a hazardous exercise for the attacker.

We can also find practical values in publications describing the realization of relay attacks. Z. Kfir and A. Wool, University of Tel Aviv, evaluate a simulated reading distance of

40 to 50 cm. From this study, I. Kirchenbaum and A. Wool build a demonstrator, easily made for less than 100\$, which is able to read a contactless card from 35 cm afar.

### ▪ ***Denial of service***

The goal of denial of service attacks is to somehow deny a given service (e.g. identification) to valid users. Denial of service attacks are easy to accomplish and difficult to guard against. They can be divided into the four categories:

- 1) Interferences in the anti-collision protocols: blocker tag and RFID guardian. If they are devices to protect the privacy of users they are also potential means for denials of service.
- 2) Reader- and card jamming
- 3) Faraday cage
- 4) Viruses and worms

The cases of the destruction of the tag or the reader and the fraudulent use of the “kill” command will be addressed in a specific paragraph.

### ▪ **Interferences in the anti-collision protocols: blocker tag and RFID guardian**

### ▪ **Anti-collision protocols**

There are two different solutions to manage the collision of tags:: either through a deterministic or a probabilistic protocol. The first one aims to calculate and indicate the exact time (linear or not) required for the singulation of every tag depending on the number of tags in the field. The second one assesses the probability to obtain the UIDs (the unique identifier code) of a certain number of tags in a given time without giving any guarantee concerning its maximum value.

### ▪ **Deterministic protocol**

The main principle of this category of protocols is that the algorithm explores the UID bit after bit exactly like the tree walking protocol until the reader encounters a collision. In this protocol, the time required to select a tag is well defined and will not vary if the algorithm is executed a second time. This protocol variant is simple to implement with logic gates and is very time efficient. For cards working at 13.56 MHz, only the ISO 14443 type A standard implements this protocol [ISO14443].

Viewed from the point of view of privacy protection, this protocol is not secure since the reader calls the different tags with their unique UID and since the request from the reader has a much higher signal than from the tag, the UID is simple to intercept. As we will see, in the other algorithm, there, only the tag emits the UID, and so the UID becomes much more difficult to intercept by a third party.

“The tree-walking singulation algorithm lets an RFID reader identify the serial numbers of nearby tags individually by means of a bit-by-bit query process resembling a depth-first search of a binary tree.

Suppose the tags in a given system bear unique identifiers of some fixed bit-length  $k$  (such as  $k = 64, 96$ , or  $128$ ).

Let  $\parallel$  denote the concatenation operator for bit strings. The set of all possible  $k$ -bit identifiers can be viewed as the leaves of a standard binary tree of depth  $k$ . The root of this tree has depth 0 and is labeled with the empty string. A node of depth  $d$  is labeled with a binary string  $x$  of length  $d$ ; if  $d < k$ , then the node has a two children at depth  $d+1$ : a “left child” with label  $x0$ , and a “right child” with label  $x1$ . (Here  $x0$  means  $x \parallel 0$  and  $x1$  means  $x \parallel 1$ .) We regard the branches of a given node in this tree as bearing labels ‘0’ and ‘1’, respectively associated with the left and right branches. Thus a node at depth  $d$  in this tree may be uniquely identified by a binary prefix  $B = b_1b_2 \dots b_d$ , representing the sequence of branch labels of branches traversed in a path from the root to the node. It follows that each of the  $2^k$  leaves in the tree has a unique associated  $k$ -bit string. We view each such leaf as representing a distinct possible tag serial number.

The tree-walking algorithm is a recursive depth-first search performed by a reader in the following way.

Let the *subtree* of a node denote all its descendents in the tree.

The reader initiates the tree-walking algorithm at the root of the tree.

Starting at a given node  $B = b_1b_2 \dots b_d$ , the reader queries all tags bearing serial numbers in the leaves of the corresponding subtree, i.e., all tags whose serial numbers bear the prefix  $B$ ; all other tags are instructed to remain silent. The queried tags reply to the reader with the  $d+1$ -st bit in their serial numbers; i.e., each tag broadcasts a '0' if it lies in the left subtree of the node  $B$ , and a '1' if it lies in the right subtree. Consequently, if there are tags in both the left and right subtrees of  $B$ , then the tags together simultaneously broadcast both a '0' and a '1', creating a collision in the broadcast bit.

In this case, when a collision is detected, the reader recourses (sequentially in turn) beginning at its child nodes  $B \parallel 0$  and  $B \parallel 1$ . If, on the other hand, the tags all reply with only a single bit  $b$ , i.e., they all lie in the same subtree, then the reader recurses on the node  $B \parallel b$ , and ignores the other (empty) subtree.

When the algorithm reaches a leaf (at depth  $k$ ), it outputs the associated  $k$ -bit sequence, which is the serial number of the tag just read. The full output of the algorithm is a list of the ID numbers of all tags within its range.

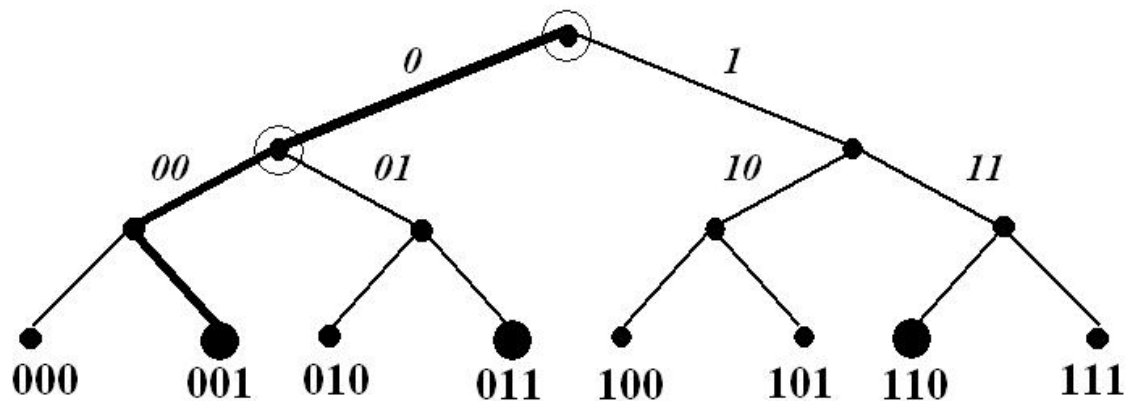
The running time of this algorithm is bounded by the product of  $k$  and the number of tags being read. In practice, a shopping cart full of goods should be scannable in a few seconds.

#### ▪ **Tree-walking example**

We provide a simple example in the following figure of how the treewalking algorithm works. This tree, which is of depth 3, has  $2^3 = 8$  tag serial numbers represented at its leaves. The prefixes associated with subtrees are denoted in *italics*. In this example, we consider three

tags as being present, the ‘001’, ‘011’, and ‘110’ tag. These are indicated by large black circles at their respective leaves.

The tree-walking algorithm here first singulates the ‘001’ tag by following the path denoted by the bold edges. At two nodes, namely the root of the tree and the root for all tags with a ‘0’ prefix, there are collisions in the bits broadcast by tags, because there are tags present in both the left and right subtrees. We denote these collision points with hollow circles. Singulation of the ‘011’ and ‘110’ tags would follow by recursion on the collision points. “[Jue03]



**Tree-walking example.** Each tag has a three-bit serial number, corresponding to a leaf in this depth-three binary tree. The tree-walking singulation protocol corresponds to a depth-first search of this tree, restricted to the leaves/ID's in use and their ancestors.[Jue03]

#### ■ Probabilistic protocol

In the 13.56 MHz range, all standards (ISO 14443B, ISO 15693, ISO 18000) implement probabilistic algorithms (sometimes called ALOHA). In this protocol, tags select a random slot number between 0 and a maximum slot number, in which to offer a reply. The maximum slot number is set in the tag as a default value, which may be temporarily overridden by a reader command. Once the tag selected its slot, the reader signals the start of each slot. The tag keeps track of the number of the current slot timed from the Wake-up command. After responding at the correct slot, the RF tag will automatically transition from the active state to the quiet state. If the tag is in the active state when the current slot number equals the maximum slot number, an increment in the current slot number causes the tag to reset its



current slot value back to one and recalculate the random slot number in which to re-offer its reply. This case arises if the response of a tag collided with another in its chosen reply slot, or the response contained an error. This cycling of current slot numbers continues until the tag response is decoded without error and it remains in the quiet state, or the tag leaves the energizing field. For flexibility, the number of slots in a round may be expanded and contracted as the tag populations grow and shrink.

#### ▪ **Example of reader-to-tag dialogue**

Upon receiving a Wake-up command, tags do not necessarily reply immediately, but begin self-selecting within a default round length a randomly chosen reply slot within this first round. The duration of a tag reply slot is dependent upon the chosen response format and the number of pages in the default reply. The number of slots which a tag expects within a reply round is dependent upon initial tag programming, but can be modified by reader commands. The start of each reply slot is signaled by the reader. An example dialog is shown in the following figure.

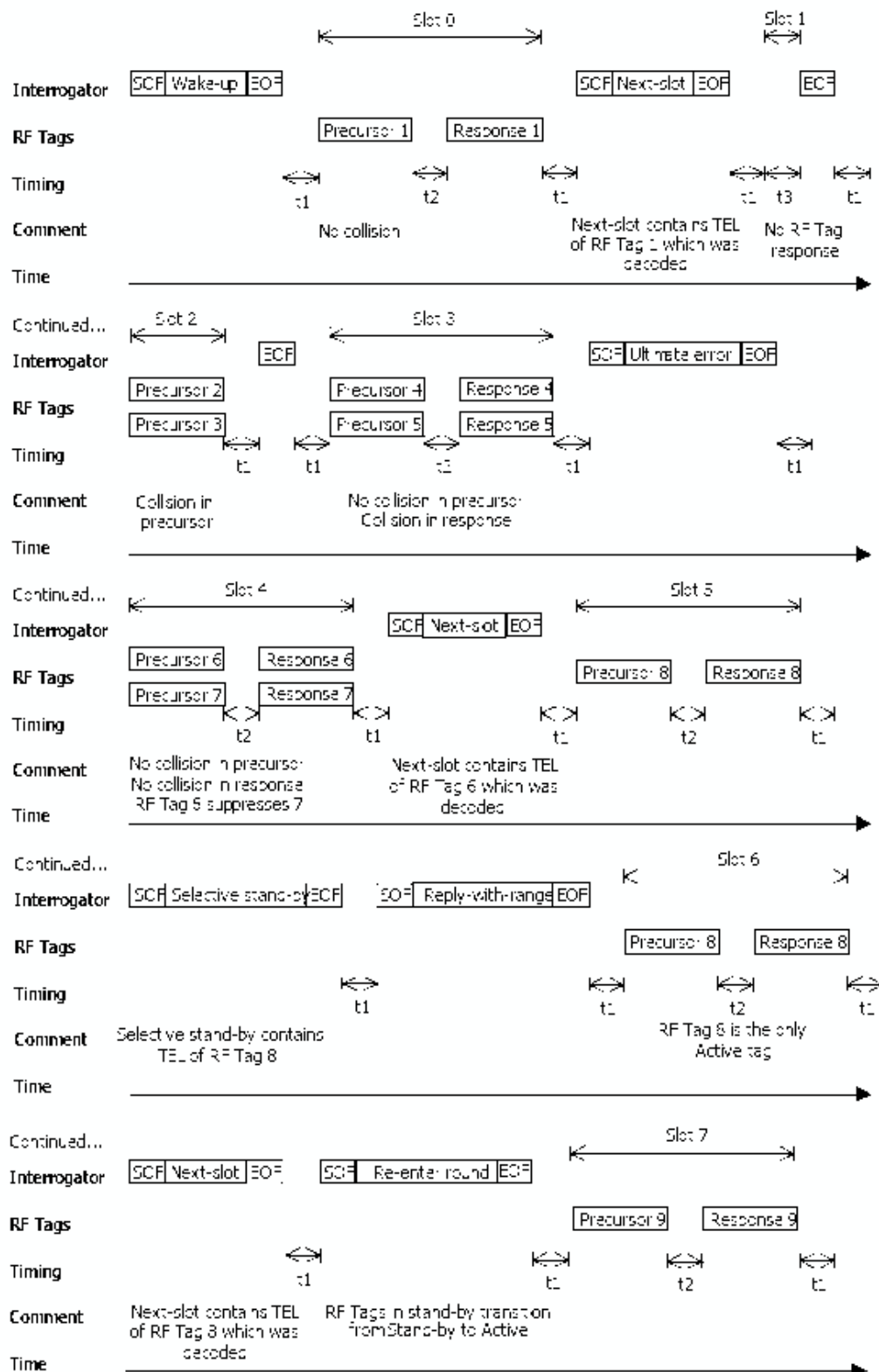
The reader issued a Wake-up command, which moved RF tags in the ready state to the active state.

RF tags read their default round size from memory and randomly select a slot in which to respond.

- Slot 0 contained a response from RF tag 1. This tag transitioned to the quiet state after the transmission
- The reader issued a Next-slot command, which contained the TEL of RF tag 1 which remains quiet.
- Slot 1 contained no response, and the reader issued a Close-slot (EOF) command.
- Slot 2 contained two responses, the precursors of which vary in their contents, so a collision is detected and the slot is closed before the main reply. The two RF tags will offer a response again in the next round (after the maximum number of slots in the current round has elapsed).
- Slot 3 contained two responses, the collision was not detected during the precursor but was detected during the CRC check of the main reply. Due to the detected collision, the reader issued an 'Ultimateerror' command. The two RF tags will offer a response again next round.

- Slot 4 contained two responses, but one is significantly stronger than the other so it appeared to the reader that only 1 RF tag was in the slot. The reader issued a Next-slot command which contained the TEL of RF tag 6. RF tag 7 will offer a response again after the maximum number of slots in the current round.
- Slot 5 contained a response of a particular RF tag which, needed to be isolated. The reader issued a 'Selective-stand-by' command, which moved RF tag 8 to the active state. RF tags 1 and 6 stay in the quiet state, while all other tags in the active state moved to the Standby state.
- At this time there is only one RF tag in the active state and there is an opportunity to request more data or program that tag. The reader issued a reply-with-range command, which causes RF tag 8 to respond with an addressed range (Slot 6).
- The reader then issued a Next-slot command, which left RF tag 8 in the quiet state.
- The reader then issued a Re-enter-round command, which moved the RF tags in the Stand-by state back to the active state.
- Slot 7 contained a response from RF tag 9.

To determine the time-slot where tags will answer, during the “inventory” command the reader emits a bit-mask that will select the tags that have this mask in their UID. Each tag associates this mask with the current slot counter. This association is then compared with a part of its UID: if they are the same, the slot counter is arrived at the time-slot where the tag should answer, else the tag should wait the next time-slot (the slot counter is then of course incremented).



**Example of reader to tag dialog**

### ▪ **The blocker tag**

Juels et al. [Jue03] developed a device that blocks the tree-walking singulation protocol and prevents intrusive readers from query the UIDs of the tags we may carry. The idea of the blocker tag is to emit both a '0' and a '1' during singulation, creating a collision and forcing the reader to branch on each and every branching point during its singulation algorithm. By emitting simultaneously a '0' and a '1' (which requires two antennas) at each node of the tree, the reader can never complete its algorithm, and so never finds out if the protected entity possess the tag with the protected UID.

As a consequence, the consumer is protected against unwanted scanning. However, the blocker can not only used as a protection device but also as a device that could potentially help an attacker generating a denial of service in a legitimate system. We can even assume that a blocker tag is always malicious since it cannot be selective and forbids the reading of one tag whereas it authorizes the reading of others. For example, if UIDs beginning with a '0' are blocked, then the reader may never get around to reading UIDs beginning with a '1'.

The blocker tag works like as a passive tag: it needs to be in the reader field for it to work, and will protect only a small volume around itself.

### ▪ **The RFID Guardian**

The RFID Guardian is an active device that can be part of a mobile phone or a PDA that the user carries with him. It can stop any pervasive reading by actively emitting a jamming signal in the sidebands of a typical RFID tag. Such a device can have multiple functions:

- Information can be sent to the reader or to the tag for secret key management, authentication, access control
- Monitoring of the RFID environment to warn of possible unsolicited reading
- Creation of collisions to prevent from the possible inquisitive reading

The RFID guardian can be a very useful tool to ensure our privacy. Naturally, by the same virtue it is also an efficient device to carry out a denial of service attack.

Whereas the blocker tag is designed to carry out a simple load modulation, the RFID guardian ([Rie106],[Rie206],[Rie105], [Rie205]) is an active device that requires batteries and thus is able to emit its own signal. As a consequence, its effective area of protection is much larger, about 50 cm in radius[Rie106]:

“The comparatively tiny sidebands have approximately 90 decibels less power than the reader-generated carrier signal, and this is the reason why RFID tag responses often have such a limited transmission range.

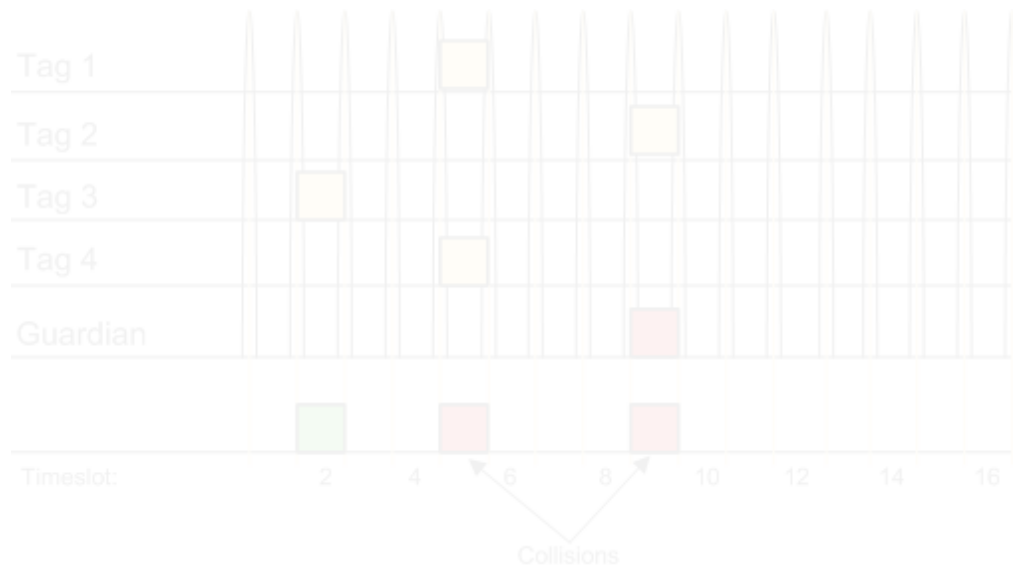
The secret to creating fake tag responses is to generate the two sideband frequencies, and use them to send back properly-encoded responses, that are synchronized with the RFID reader’s clock signal. The simplest way to generate these sidebands is to imitate an RFID tag, by turning on and off a load resistor with the correct timing. The disadvantage of this approach is that passive modulation of the reader signal will saddle our fake tag response with identical range limitations as real RFID tags (~10 cm for our test setup).

A superior alternative is to use battery power to generate the two sideband frequencies. These super-powerful sidebands are detectable at far greater distances, thus increasing the transmission range of our fake tag response.

The RFID Guardian prototype utilizes the “active” tag spoofing approach. The following figure shows the signal generated by our tag transmitter. The spoofed “sidebands” are transmitted at a power level roughly equal to the reader’s carrier signal. This has increased the range of our fake tag responses – from 10 cm to a half meter away!”

This smart jamming can also be selective and can make the reader think that certain tags are absent from its field. Thus, in a ALOHA anticollision protocol, the RFID Guardian is

able to determine the time-slot where those tags will answer and then to emit a jamming signal in those time-slot to create a collision and to prevent from the inquisitive reader to understand the UIDs of the protected tags.



***Selectively jamming of Tag 2 with the RFID Guardian. Since we increase the number of collisions, the singulation protocol is slowed down but the reader will be able to read all the permitted tags contrary to the blocker tag. However, in case of the use by an attacker, it can be imagined that a collision is created in every time-slot and in every round. Then, a denial of service is generated with a full blocking of the reader [Rie106].***

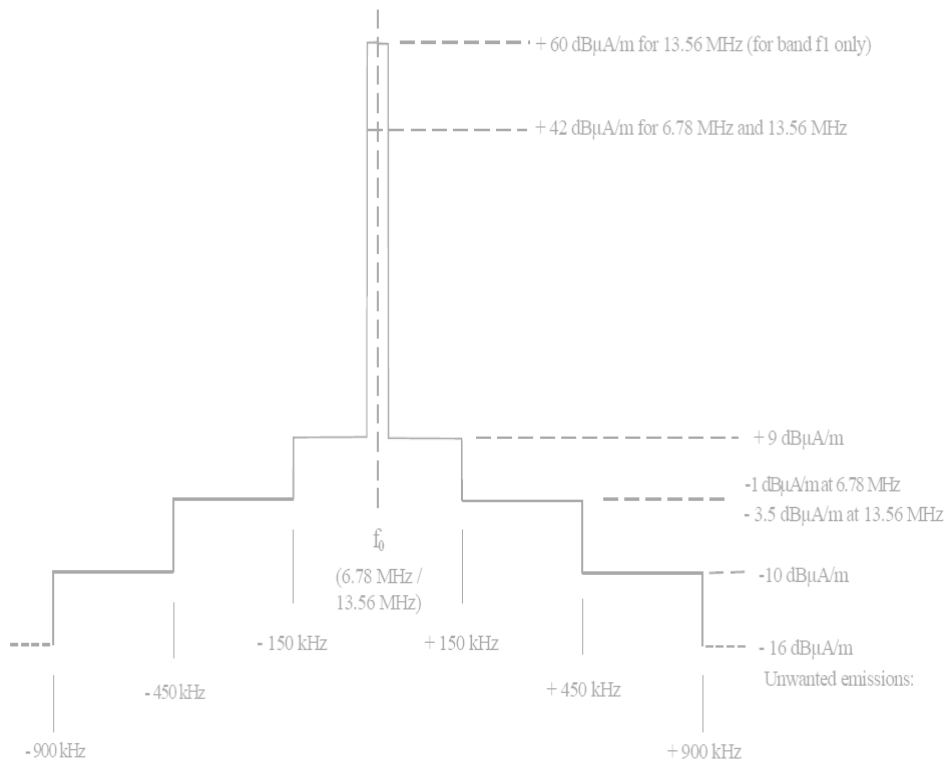
#### ▪ Reader and card jamming

The jamming attack is often mentioned in numerous papers without being fully detailed. The idea is to emit a signal in the same bandwidth as the reader or the tag in order to blur the transmission between the reader and the tag.

Considering that this attack presents no ingenuity in the noise emitted or in the period it is emitted, the only constraint is to flood the reader or tag signal in a higher level noise. The maximal level of emitted magnetic field is already restricted in international agreements. The ETSI EN300-330 describes a template of magnetic emission at 10 m around 13.56 MHz. According to the following figure, it is illegal to emit more than 20 dBμA/m at 10 m in the 13.56 MHz frequency.

As a consequence, any attacker that is able to pass this limitation is sure to create an efficient jamming of a RFID reader. Exceeding the standard does not necessarily mean that

the jamming signal requires a lot of power, however. If the noisy emission is in the exact bandwidth of the reader signal, only a few watts (1 to 2 W) are enough. To blur a tag signal is even easier since its signal is much lower than the reader's.



**ETSI EN300-330 13.56 MHz magnetic field strength limit at 10 metres measurement distance. A higher signal in the bandwidth will blur the communication.**

## ▪ Shielding and using a Faraday cage

A basic solution to prevent from a reader to read our contactless card or RFID tags is to shield them by confining them in a wallet made of a metallic sheet or mesh. This wallet plays the part of a Faraday cage blocking the HF and UHF radio signals of readers. To be efficient against HF electromagnetic waves, the thickness of the metallic sheet should be greater than 20  $\mu\text{m}$  for a metal with a good conductivity like copper or aluminum. Considering the metallic mesh, the period of the grid should have a length around half of the wavelength.

This solution is cheap, efficient and is not based on a complex technology. As a consequence, it is a very reliable way to ensure the security of contactless devices while not in use. There exists a large supply of this kind of wallets on the Internet [Mobi],[Dif],[Ste].



***Wallets with metallic shield***

#### ▪ **Viruses and worms**

The announcement of the possibility to convey viruses and worms in RFID systems unsettled the community of specialists in 2006 [Rie306]. This kind of denial of service is not based on a weakness of the physical contactless link but it points out a certain number of faults in the middleware that could potentially be exploited by RFID tags. Three fault sources were investigated by Riebeck:

- Buffer overflows: “RFID tags can exploit buffer overflows to compromise back-end RFID middleware systems. This is counterintuitive since most RFID tags are limited to 1024 bits or less. However, commands like 'write multiple blocks' from ISO-15693 can allow a resource poor RFID tag to repeatedly send the same data block, with the net result of filling up an application-level buffer. Meticulous formatting of the repeatedly sent data block can still manage to overwrite a return address on the stack.” [Rei306]. To prevent such an attack, the developer of the middleware should always be in control of the size of the message the tag sends.
- Code insertion: “RFID tags with data written in a scripting language can perform code insertion attacks on some back-end RFID middleware systems. If the RFID applications use web protocols to query back-end databases (as EPCglobal does), there is a chance that RFID middleware clients can interpret the scripting languages (perhaps because the software is implemented using a web client). If this is the case, then RFID middleware will be susceptible to the same code insertion problems as your typical web browsers.” [Rie306]. Normally EPC RFID tags send only their UID that is not interpreted as executable code, but as pointer in a database. Therefore, if the middleware is well implemented, malicious code insertion cannot be carried out.
- SQL insertion: SQL injection is a type of code insertion attack that tricks a database into running SQL code that can be (at least partially) controlled by the attacker. The paper by Riebeck shows that if a RFID tag is able to send SQL commands (it would be more accurate to say if a middleware interprets the tag UID as a SQL code) then it



is possible to change the database such that it will replicate the malicious code into any RFIDs it encounters in order to spread the virus to other vulnerable SQL backend databases.

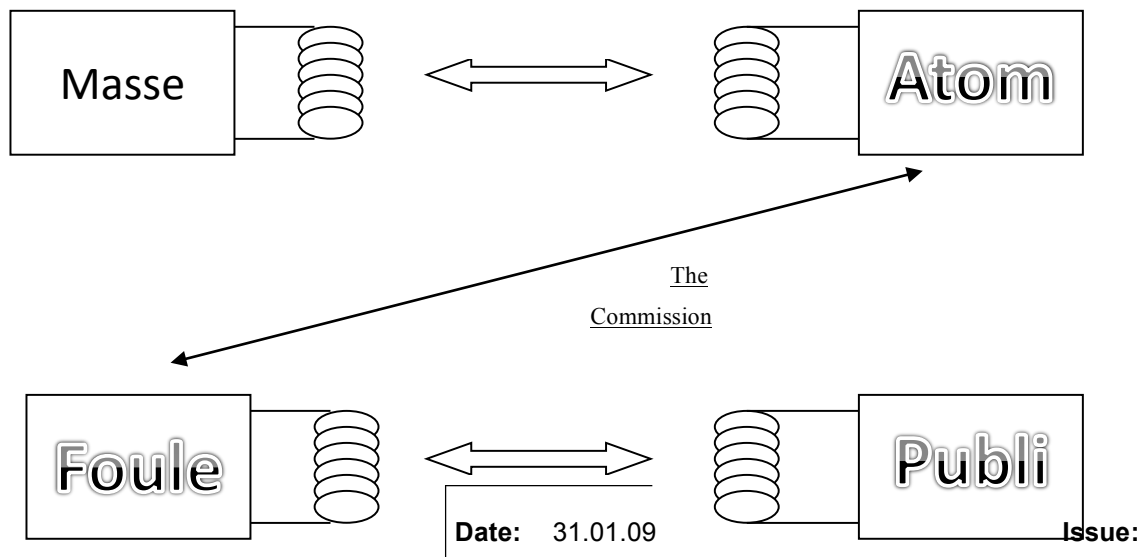
To guard against these types of attacks, the contents of an RFID should never be trusted by the middleware in RFID systems.

#### ▪ ***Relay Attack***

The relay attack is based on a specific weakness of the contactless smartcards or RFID tags: the possibility to activate the device without the consent of the user. Currently, there exist no RFIDs that can be simply switched off by their owners. Thus an attacker can access the card discreetly, without knowledge of its owner, and relay information through a communication link between the card and a remote reader. The reader will assume that the card, and by implication the user, is in close vicinity and will allow secure transactions to take place that should only be carried out by consent of the cardholder.

Even if the attacker is not able to view in plaintext any communications that take place, this is not needed as long as he can continue relaying the respective messages. The attack can be further enhanced by relaying the initial authentication sequence after which subsequent data is modified before relay.

Relay attacks involve two different devices and as a consequence two attackers that must coordinate their actions, except if the relay is really short (an arm's length for example). The device that will skim the data off the attacked person is named the "leech", though the term "mole" is sometimes also used. The leech is linked via the relay to the "ghost" (also named "the proxy"), a fake card that will reproduce the data of the genuine card.



CHF

Principle of the relay attack

The threat of the relay attack could be understood by the scenario provided by [HR07] and involving the Czech e-passport. A Czech visitor in a hotel in a foreign country leaves her passport at the hotel's reception. Having physical access to the passport (and its MRZ – Machine Readable Zone), the receptionist can access and copy all of the public data, i.e. namely the files DG1 (copy of Machine Readable Zone), DG2 (biometric photography of the holder), DG15 (public key for AA) and EF.SOD (digital signature of the DG files by national authority). Leaving the passport at the reception, one can cross the border identifying himself with the victim's passport in the following way. The attacker passes the Basic Access Control procedure simply by using the known MRZ data and provides the copy of DG files to the reader at the border. Consequently, he enters the AA protocol by receiving the AA challenge and relays it by an intermediate channel (e.g. TCP/IP) to a device at the reception which transmits it to the victim's passport. As the reader at the border has to be standard compliant and as a consequence has to wait 5 seconds for the answer, there is enough time to relay the passport's answer back to it.

To define the features of a relay attack, three different parts should be characterized: the leech, the ghost and the relay between them. The leech is a skimmer that has to activate and power the attacked contactless card and to communicate with it. Skimming a card is an attack in itself and is already intensively discussed in this document. The leech-to-tag reading distance could be up to 50 cm [KW05] by supplying enough current in a specifically designed antenna and by employing intelligent signal processing.

The ghost is able to eavesdrop on the communication with a genuine reader and to talk back to it. The eavesdropping on the communication is also well documented in this document. Concerning the fake card response, active modulation could be used instead of a load modulation that requires a close coupling and so a short range. [KW05] assesses that the ghost-to-reader distance could be as far as 50 meters. However, no realization lets us confirm such a distance. The RFID guardian [Rie106] that has to provide the same functionality has a 1 meter operating distance.

The ghost and the leech are not specific to the relay attack since they are used for skimming or eavesdropping on the communication. The main challenge to be overcome during the relay attack is the fact that relaying data introduces delay into the system. It is therefore pertinent to consider the timing constraints in the original system. ISO 14443-3 specifies timing requirements to maintain bit synchronization during the anti-collision process. Response time is specified as  $(n \times 128 + 84) / f_c$  if the last data bit sent by the reader was '1' and  $(n \times 128 + 20) / f_c$  if the last data bit sent was '0'. Response times are calculated using  $n = 9$  for REQA and SELECT commands, and  $n \geq 9$  for all other commands. The minimum timeout defined for REQA commands is  $7000 \times f_c - 500 \mu s$ . ISO 14443-4 specifies the FrameWaiting Time (FWT) as  $(256 \times 16 / f_c) \times 2FWI$ , where FWI is a value from 0 (FWT = 300  $\mu s$ ) to 14 (FWT = 5 s) with a default of 4 (FWT = 4.8 ms). The FWI value is defined by the card in its ATS response. The Frame Waiting Time defines an upper bound, and a modern communication channel should be able to forward a few data frames in 5 s. Therefore the anti-collision timing constraints are more of a concern, especially since the responses are ordered to a bit grid, resulting in the card only answering when the information is due, after

91  $\mu$ s and 86  $\mu$ s respectively. An idle reader transmits REQA commands periodically and as a result the ghost held to the reader requests information from the leech with the same regularity until the leech is within range of the targeted card.

The minimum response timing (86  $\mu$ s) opens the door to a large number of communication protocols and modulations: GSM, TCP/IP with WIFI, in authorized radio bands. The more useful is the NFC standard developed for mobile phones where the three required components are available in the same device: the RFID reader, the RFID card and the communication relay with GSM (or even WIFI in smartphone) [KW05]. All those communication protocols always implement a modulation and bit coding that are different from the RFID standards. Therefore they require adapting a stream bit coding that can take time. [Han05] shows in their implementation that this double adaptation (from the ghost to the relay and from the relay to the leech) introduces a timing delay from 15 to 20  $\mu$ s that does not disturb the service.

The different developments point out the low cost of such an attack: it could require less than 200 €. However, this cost could be drastically reduced if the relay is just a wire that transmits along a short distance (around 1 meter) the bitstream with only an amplification of the signal, since an adaptation of the modulation and of the bit coding is no longer required.

With its capability of attacking from a long distance without the consent of the user and of bypassing the encryption of the contactless transaction, the relay attack appears to be one of the main threat for RFID systems.

In literature, we distinguish two kinds of relay attacks:

Mafia fraud: prover (the tag) and verifier (the reader) are honest. The attacker only relays the messages.

Terrorist fraud: prover is honest but the verifier collaborates with the attacker.

- ***“Man in the middle” attack***

“Man in the middle” attack is often mistaken for relay attack. They are indeed similar but with the distinctive feature that in this attack the bits stream can be modified in during relay. Since the relay implies the adaptation of the modulation and of the bit coding by the leech or the ghost for its use, it is not a challenge to change arbitrary bits. This additional feature may take time but it will always be shorter than the 5 seconds timeout of the reader. However, by changing the data transferred, the opportunity to bypass the encryption of the transaction that exists in the relay attack disappears. Thus, if the communication is ciphered, the attacker should know the secret keys of the algorithm to change the data. Two stages are then required: the decoding with the known key (that requires another kind of attack to be retrieve), the coding of the modified plaintext. The 5 seconds timeout is obviously enough to compute any cryptographic algorithm even with asymmetric keys.

- ***Side channel attacks on the contactless interface***

In the previous sections, we have presented specific attacks related to contactless technology. We have to mention other types of attacks which apply to both contact and contactless cards: the so-called Side Channel Attacks (SCA).

SCAs exploit the behavior of the chip during computations. Indeed, analyzing power consumption, electromagnetic emissions, calculation time, can reveal some information which can be helpful for recovering secret information for instance the secret key(s) contained into the chip memories.

- **Power Consumption Analysis**

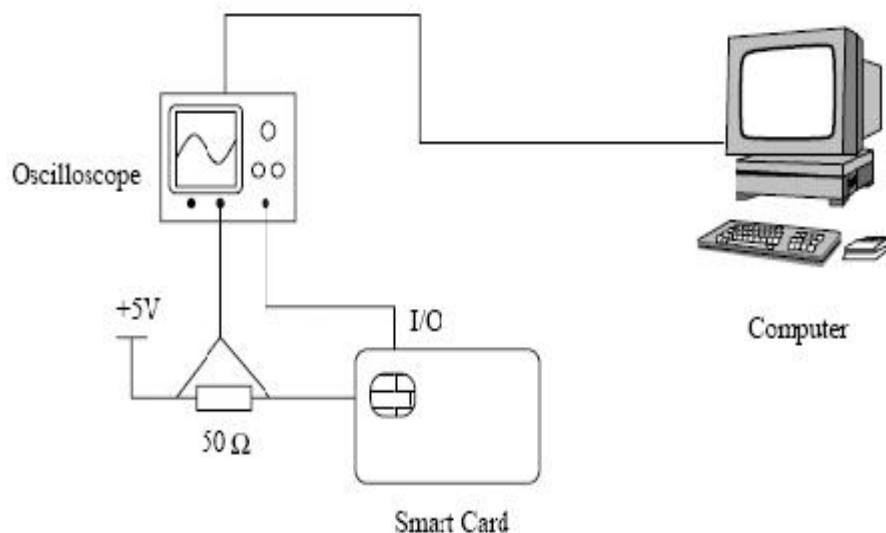
In 1996 Kocher introduced the side-channel attack (SCA for short) based on execution time measurements [to fill].

In 1998 [KJJ99], Kocher, Jaffe and Jun described two new methods using the measure of power consumption for retrieving secret keys: SPA (Simple Power Analysis) and DPA (Differential Power Analysis). These attacks are based on the following idea: the power consumption of a chip mainly depends on the performed instruction and on the manipulated data.

They threaten any naïve cryptographic algorithm implementation, a numerical oscilloscope is necessary.

Indeed an electronic device is composed of thousands of logical gates which switch differently depending on the executed operations. The power consumption depends on the executed instructions and the manipulated data. Thus by “simply” monitoring the power consumption of the device on an oscilloscope (eventually followed by some signal processing) information on some secret data can be gained from this signal analysis. Since 1998 the field of power analysis has been deeply investigated,

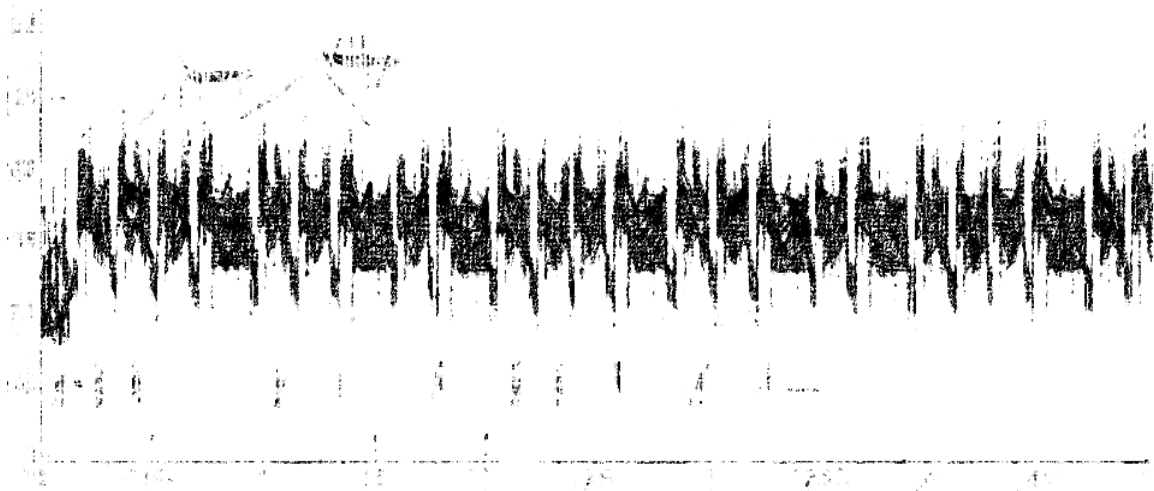
Measurement bench:



#### ▪ Simple Power Analysis

SPA is a power analysis based on a single trace : the attacker can find information just by analysing carefully the curve representing the execution of a cryptographic algorithm. Usually SPA is particularly efficient against algorithms of which the execution path depends on the secret parameters. Therefore not properly protected implementations of asymmetric

algorithms are especially vulnerable. The following picture shows how to recover an RSA secret key by conscientiously inspecting the trace.



*SPA on RSA*

In the square and multiply algorithm, a square operation may be followed by a multiplication according to the key bit involved. However, a multiplication is always followed by a square. These observations allow linking a pattern to its corresponding operation and then retrieving the involved bits.

Indeed two consecutives squares on the curve imply the exponent bit was 0 otherwise it is 1.

Simple Power Analysis can be applied to any kind of computation, any algorithm can be concerned by such a threat: ECDSA during the scalar point multiplication, DSA during the exponentiation, Diffie-Hellman computations, DES, AES during the key scheduling operations, etc.

#### ▪ **Differential Power Analysis**

DPA is a technique where power traces are combined in a statistical manner to obtain information about the secret parameters manipulated by the algorithm. A DPA may require several hundreds of power consumption traces corresponding to the computations of the same

algorithm. Of course, DPA works only if the key or the secret parameter is unchanged for all these executions.

Let us see how perform this attacks on the DES (Data Encryption Standard) algorithm.

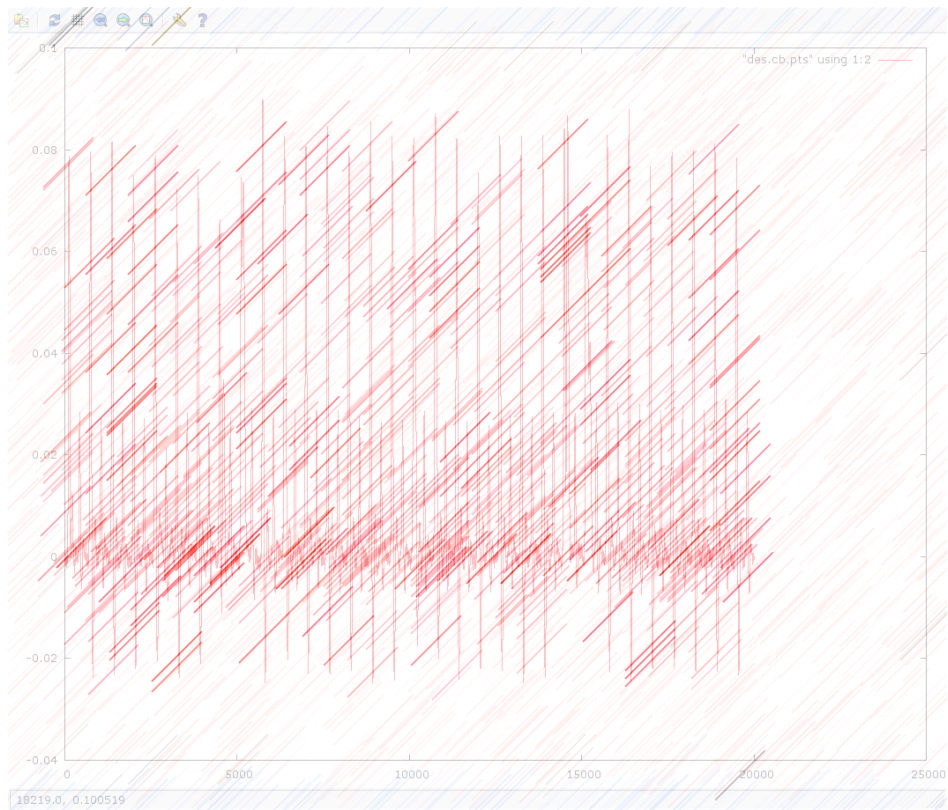
This algorithm operates data in sixteen rounds. During the first round, it compute a value  $S(M \oplus k)$  where  $k$  is a 6-bits subkey,  $M$  is a 6-bits fragment of the message after the Initial permutation  $IP$  and the expended permutation  $EP$ ;  $S$  is a substitution table which takes a 6-bits input and returns a 4-bits output.

For more detail we advice the reader to read the document [FIPS ...].

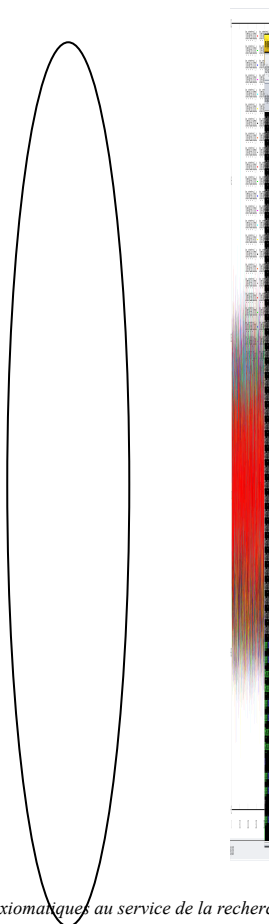
We try to find the key by 6-bits fragments, we proceed as follows.

- Generate  $N$  power traces corresponding to the execution of the algorithm for  $N$  different input messages. ( $N$  is a “large” number  $>100$ ).
- A 6-bits subkey can take only 64 possible values.  
For each subkey guess  $k_i$  :
  - Simulate the algorithm by computing  $S(M \oplus k_i)$  with all the  $N$  messages  $M_j$ .
  - Apply a selection function  $D$  (for instance one bit of  $S(M \oplus k_i)$  which gives a value 0 or 1 to split up the traces into two sets  $E_0$  and  $E_1$ .
  - Compute the differential trace  $E$ : it is the difference between the average of the traces of  $E_1$  and the average of the traces of  $E_0$ .
- We thus obtain 64 differential traces. The correct guess corresponds to the trace which presents the highest peak.





*Power Curve of a Hardware single DES execution*



Attacks are possible at points where the outcome of a calculation can be predicted, by using known information (for example input and output) and information for which all possibilities can be checked (for example a small part of the key).  $D$  is a function that calculates the

predicted intermediate value at the attack point and divides the traces according to this output.

DPA is based on the fact that  $E$  will be flat (low) where the power usage is independent of the outcome of the function  $D$  (i.e. places where the key is not being used or where the key was guessed incorrectly). For the correct guess, where the power usage is dependent on  $D$ ,  $E$  will be “bigger”, a significant peak appears for the correct guess.

Many improvements of DPA have been proposed, one of the most significant is the CPA for Correlation Power Analysis.

This technique has been introduced on symmetric algorithms by Brier, Clavier and Olivier in [BC004]. More recently Amiel, Feix and Villegas [AFV07] studied the Correlation Power Analysis (CPA) with a leakage model to most part of the common asymmetric algorithms and presented successful new attacks on public key implementations with different coprocessors.

This technique allows obtaining secret information with few curves, for instance on some chips 40 curves only can be necessary to recover the secret key.

#### ▪ **Electromagnetic Analysis**

Since any electrical current flowing through a conductor induces electromagnetic emanations, it seems natural to expect such emanations to leak information in the same way as the power consumption. This idea of electromagnetic attacks was first introduced by Quisquater and Samyde in [QS01].

The attacker first de-capsulates the chip by removing the top layers protecting it. Next, the surface of the chip is scanned to find the best location for electromagnetic measurements.

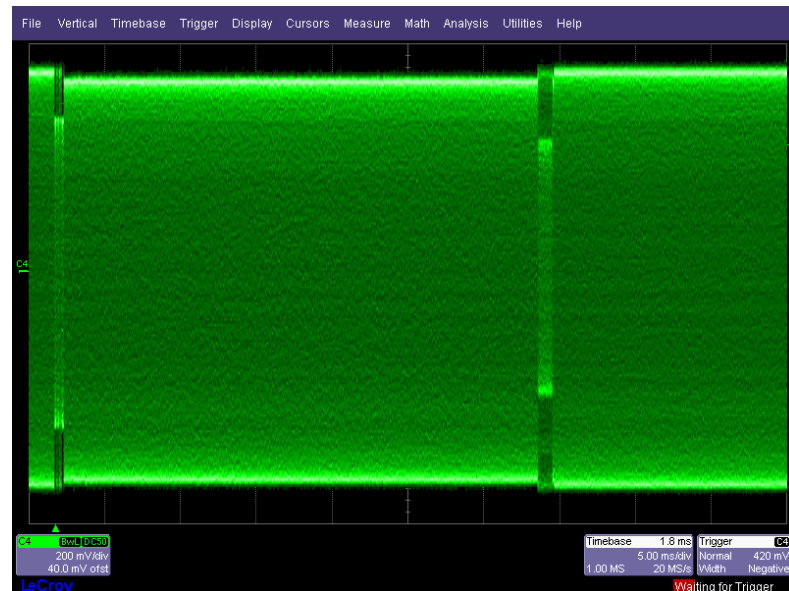
These very fine measurements require a specific tiny probe linked to an oscilloscope which transforms local electromagnetic emanations into measurable power curves.

Then, EMA is quite similar to power consumption analysis, techniques can be adapted to EMA: SEMA (Simple Electromagnetic Analysis) and DEMA (Differential Electromagnetic Analysis)

## ▪ Radio Frequency Analysis

There is another technique used exclusively in contactless technology: RFA (Radio Frequency Analysis).

By measuring with an antenna the electromagnetic field consumed by the card one can obtained same kind of information than with power consumption curve and process the same attacks.



*Radio Frequency Field Measured*

This figure shows the RF which can be measured between the card and the reader. By focusing on some part of this curve and using signal processing techniques same a curve related to the cryptographic operations can be obtained.

Thus there are few differences between contact and contactless cards when confronted to side channel attacks.

The main one could be the following: to process to SCA on contact cards the card must be connected to a reader whereas a RF field can be measured regarding a certain device of the reader and the chip. Thus SCA could be processed at distance and not seen by the card owner.

#### ▪ ***Differential Fault Analysis and Fault Injection Attacks***

In the 1990s, we observed that fault injections and perturbations into a component during computations could lead to information leakages and reveal sensitive data.

However use for analyzing embedded cryptographic implementations has first been done in 1997 when D. Boneh, R. DeMillo and R. Lipton [8] published the first theoretical fault attack. This is known as Bellcore attack. Thereafter Lenstra wrote a short memo [22] to shortly improve this attack. In case of computation error, the Bellcore researchers showed how to recover the secret factors  $p$  and  $q$  of the public modulus  $n$  from two signatures of the same message: a correct one and a faulty one; Lenstra showed that only one faulty signature is required when the message is also known. In 1997, E. Biham and A. Shamir [6] presented the first Differential Fault Analysis (DFA) on a symmetric algorithm applied to the Data Encryption Standard (DES). Those attacks are seriously taken into account during the design of secure products since very realistic and easy to mount in practice. Thus any implementation can be threatened by fault injection techniques. As for power analysis many researches have been conducted in this domain.

Indeed integrated circuits are able to properly run in limited environmental conditions (power, temperature, frequency). When the circuit is operated out of this normal condition some data can be corrupted. If operating conditions are far enough from the expected one, the circuit will completely fail. If the operating conditions are just at the border of the normal one or goes out of the border for just a very short time, some

errors can be induced inside the circuit. If these errors occur during a cryptographic computation under certain conditions that will be presented hereafter, they will permit to recover the secret key.

There are several techniques available to perform a fault attack. The most common are the following ones:

- Glitch attacks: variations in the current (contact cards) or in the RF field are done to perturb the chip behavior and obtain abnormal behavior.
- Light attacks: the effect of light will be a generation of carriers in the active part of the circuit. If this generation is sufficient, it can cause an inversion of the state of the closest gates. Another effect that can be induced by a laser pulse is a local heating of the device.

#### ▪ ***Attacks on multi interfaces smartcards***

#### ▪ **Coexistence of different interfaces**

The present description limits itself to the case of multi-interfaces smartcards with a partial or total sharing of the resources (memory & MMU, CPU, Crypto processors, Random Number Generators...) on a shared memory configuration or on a single memory configuration [eESC]. In such a case, the different interfaces can be managed in a:

- Dual mode: The different interfaces are mutually exclusive and, during a session, only one of the different interfaces can be activated. This mode is managed with the definition of priorities between the different interfaces. The definition of the priorities can be defined in a static way (an interface is always considered as priority) or in a dynamic way (the first activated interface and opened session define the priority interface).
- Combi mode: The different interfaces can be activated in the same session. In such a mode, the management of the commands received in the different interfaces can be managed in a interleaved way (sequential management), a simultaneous way (the CPU is shared to process simultaneously the different commands received by the different interfaces) or following a predefined priority structure (an interface is defined as having priority over the other and a command received on this interface induce the closing of other pre-opened sessions)

Increasing the number of interfaces induce more complex designs in a way that every basic function (energy supply, re-initialisation triggers, IO transfers...) has to be possibly transferred through each interface. In this context, an attacker has the opportunity to use the weakest interface or to use different interfaces in the same session for non invasive attacks (to spy the chip activity, to use it in a non anticipated way or to stress the chip to get wrong computation or software rerouting). The philosophy of every attack is the same as the ones generally encountered in contact smartcards [CC] but the numerous interfaces increase significantly the field of the possible attacks.

Those attacks have to be considered whatever the mode that allows to manage the different interfaces (Combi mode or Dual mode)

Some basic examples are now described in order to illustrate the possibilities induced by the coexistence of different interfaces:

- Spying attacks: For some reasons of energy consumption, it happens that some counter measurements against spying statistical attacks (DPA/RFA like attacks) can not be implemented when using specific interfaces. Such constraint can be used to perform an efficient attack and decrease the security robustness of a chip.
- Re-initialisation operation: In a case of a chip that would not be well designed, a cold reset in contact mode could not be followed by effect if the chip is equipped with a contactless interface and when there is a sufficient electromagnetic field in the chip surrounding.
- Perturbation attacks: The energy supply of the chip can be made by different channels. The energy transfer is not based on the same electronic blocks and then the sensitivity to power glitches of the chip can be different as a function of the used interface.

#### ▪ **Crosstalking attack**

Such attack has only to be considered in the case the interfaces are managed in Combi mode.

Such attacks are taking advantages of weaknesses and flaws (if any) on the protocol or in the way the interfaces are managed in combi mode (simultaneous access to a session via different interfaces). The main weakness happens when a shared resource can be accessed by different interfaces in a same session and if controls (hardware, operating system or software/application layer) are not sufficient to avoid such attack.

A basic example of this kind of attack is now described:

- First thing first, a session is opened by an authorised user in contact mode and a authentication process is validated via this interface.
- Next, an attacker sends a command to the chip (that should be refused by the chip if the session had not been opened before by the authorised user) with the help of the contactless interface. If such operation is possible, the attacker has access to confidential services/data without the consent or awareness of the cardholder.

## ▪ ***Destruction***

This attack consists in making definitively unusable a contactless card, but it can concern the reader, too.

Although this attack threatens contactless system availability, it is different from the denial of service attack because once performed, it is irreversible.

Destruction is considered as an attack when it is practiced without the holder's consent but it is privacy protection if a card is definitively destroyed with the consent of its holder in order to protect its data from any future attacks.

We can distinguish two destruction types: material destruction and software destruction. As this state of the art talks exclusively about contactless RFIDs, only distance material destructions are treated.

## ▪ **Material destruction**

Destruction appears rarely in literature unlike chip self-destruction in response to chemical, mechanical, etc. attacks practiced directly on the chip and described in patents [BRE1].

An article published by « Pirate magazine », in February 2007, presents schematics for detecting contactless cards presence in a field and for generating electromagnetic pulses able to destroy a chip at a short range. The schematic describes a tool that needs power from a power outlet, and so its usefulness is limited.

The BSI report compares contactless chips with EAS (anti-theft) which can be used at stores' cash desks. A strong magnetic field can induce a high voltage on the chip and an electrical failure or a warm-up of input stage. Protections, such as Zener diodes or self-healing fuses, can be integrated but the effect will always be limited by the available chip area. There is no absolute protection against destruction by electromagnetic field. On the other hand, generating a strong magnetic field requires a large instrumentation [RI1].

Some publications give the microwave oven as a tool for destroying a contactless chip. Of course, this method can only be used to destroy one's own tags.

- **Software destruction**

As in the previous case, there aren't many publications on this subject. Software destruction needs commands allowing definitive card inhibition of the card, just like the "kill" command in the EPC standard. It is quite easy to protect against this threat using an authentication process but the RFD then becomes more complicated. We must use either keys, passwords or other methods to authenticate the destructive command. [BSI1] [ERU1].

- ***Counterfeiting, substitution and replay attack***

Numerous attacks on contactless cards or RFID tags require counterfeit cards. For example, a skimming attack can enable the dumping of the entire memory of the attacked chip and then a duplication of this memory in a customized card could be a real security hazard. Thus, as anybody can easily buy on the Internet any card from any manufacturer (ST, ASK, TI,...), that has a microprocessor which can be easily programmed, this hazard is very real.

It is also possible to substitute a RFID tag on an item with another tag of a cheaper item or with a tag that is totally reprogrammed with an aforementioned chip. The difficulty is then often to reproduce the packaging of the tag that can contain holograms (e.g. credit card), signature, magnetic tapes, barcode and optical signatures. The solution is then often to tamper with the chip and replace it with a reprogrammed one.



## ■ Designing for privacy : a social technical standpoint

---

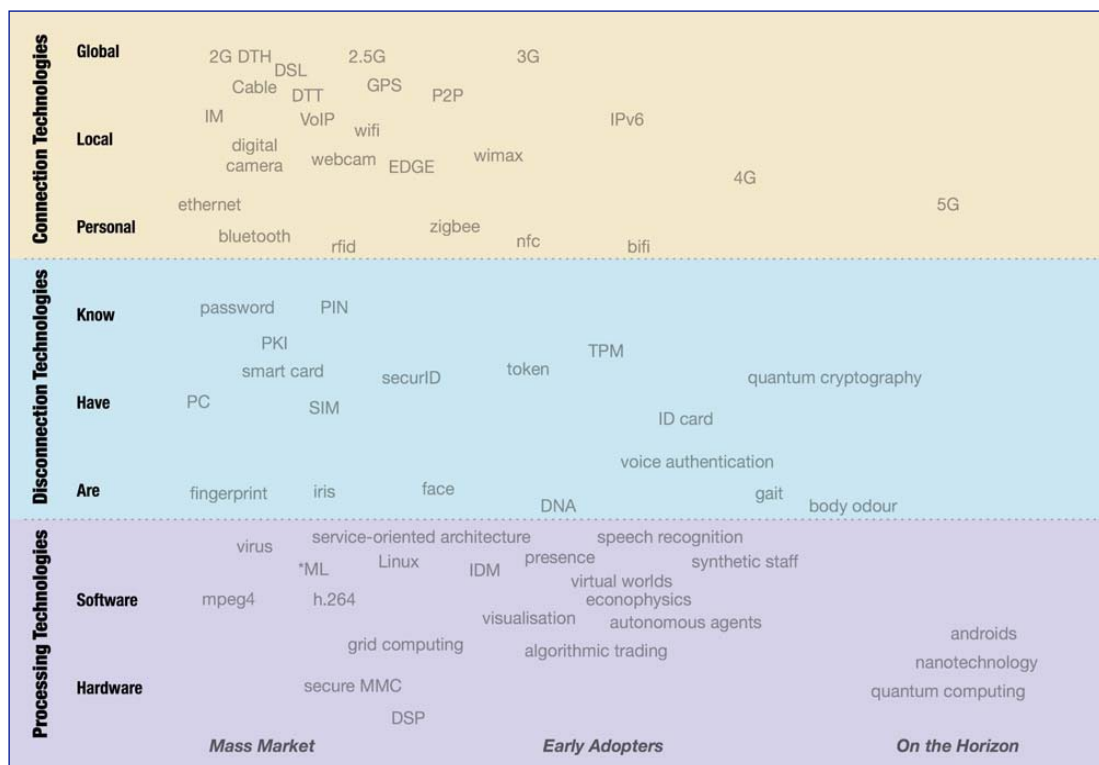
*“Technology is culture made obdurate. It embodies, fixes, stabilizes social relations. It provides mass and momentum to social systems. In studying the production and use of technological artefacts, we study the production and use of lasting cultural distinctions and relations. In studying the problem of socio-technical stabilization, we study “the problem of securing the social order”. Technological systems not only secure and fix social relations; they are products of social relations. Institutionalized resources, relationships, and courses of action are brought to bear in order to shape technological systems that will in turn constitute and facilitate new institutionalized resources, relations, and of course action. Technical systems, then, are essentially social, and social systems are essentially technical. Actors use various resources in order to shape and influence socio-technical change. These may include economic resources, such as patents, market power, or the creation of more cost-effective processes.” Philips [34].*

Beyond this battle about the normative legitimacy of privacy protection, The Royal Academy of Engineering [35] tries to forecast three different future models, based on their distinction between **connection technologies** (technologies that move data around), **disconnection technologies** (technologies that control access to data) and **processing technologies** (technologies that extract information from data):

- **Big Brother:** In this model, both connection and disconnection technologies remain fragmented and beyond central control. In contrast, continued advances in processing technologies mean that it is relatively simple to scan and record all forms of communications: thus, a 'Big Brother' can easily exist. But the implicit mental model of Big Brother that is invoked is curiously old-fashioned, because it is Orwell's vision that has become so dominant. This vision is rooted in a post-war perspective with a bleak political future, where technology is used to create giant databases so that a centralized government can exercise control of society. However, the danger more likely nowadays is that if technology continues to evolve along current lines, 'Big Brother' will end up being more powerful than Orwell envisaged (in the sense that we will have far less individual privacy), though it may not be government that will be empowered. In a world of matchbox-sized camcorders and camera-phones, of always-on broadband and RFID, ordinary people (not a government agency, supermarket or

the police) will be the nemesis of privacy. The Internet has the potential to democratise and decentralise Big Brother, as it democratises and decentralises many other phenomena; Big Brother may be 'us', not 'them'. This form of 'ground-level' surveillance has been called “sousveillance”. By its nature it is not under control and there are no transparently obvious ways to bring it under control. If a major retailer were to abuse customers' privacy, those customers could at least look to an industry code or to a watchdog to do something about it. If a government department does something irresponsible with personal data, there is recourse to complain to an ombudsman. But if someone with a camera - phone takes a picture of a businessperson going to a sensitive meeting and then e-mails it to a competitor, it is hard to imagine what could be done about it.

- **Big mess:** This is close to the current situation, where connection dominates and both processing and disconnection are uncoordinated (except in certain specialized subsectors such as defence). Individuals and organizations find it difficult to disconnect and even those organizations with legitimate requirements for processing find it hard to bring together the information they need.
- **Little sister:** In this model, disconnection technologies are widely used in a co-ordinated manner: personal data is routinely encrypted and managed in a secure fashion, so co-ordinated connectivity does not threaten it and even substantial processing resources are not a day-to-day threat. This leads to Little Sisters who, by themselves, watch over only a fragment of a person's identity, but when co-ordinated can reveal all.



Royal Academy of Engineering's technology timeline [35]

Then, considering the COPRIM project under the light of these three future models gives us some interesting points of reference:

- First, it enables us to understand the CPM Manager as a **disconnection technology**<sup>1</sup> aiming at giving the user more control on the NFC as a connection technology.
- Second, it allows us to think that the most innovative part of the project lies on its ability to **echo the little sister scenario**. Indeed, this is particularly true when we consider the peer-to-peer mode of communication in NFC technologies.
- Third, it stresses out the **substantial shift of the individual status**: from a potential prey to be protected, it becomes an **active entity that can dynamically act upon privacy spheres** – his or hers but also those of others. This latter phenomenon also turns the individual into a potential threat (cf. “sousveillance”). This process indirectly put the engineer in charge with a design dilemma: would giving the user the “*ability to express and rely upon a set of guarantees that a system may make, explicitly or implicitly, about its treatment of user data and other resources*” [2] imperil the user’s privacy?

<sup>1</sup> It is clear that the three categories used by the Royal Academy to describe technologies are not to be understood as exclusive. They rather stress out the main trait of one technology.

By raising this question, we do not intend to demonstrate that designers are the only ones responsible for tackling privacy concerns as demonstrated in the previous section. However, the goal is to stress, along with Bellotti and Sellen [8], that: *“The need to understand and protect personal privacy in sophisticated information systems is becoming critical as computing power moves out of the box-on-the-desk into the world at large.”* Ubiquitous computing urges the need to design for privacy as the Royal Academy of Engineering declares: *“There is a challenge to engineers to design products and services which can be enjoyed whilst their users' privacy is protected. Just as security features have been incorporated into car design, privacy protecting features should be incorporated into the design of products and services that rely on divulging personal information.”* [35].

The next section will demonstrate that designing security is not a value-free act. Whereas *“data security is value free (we might make the wrong sort of communications secure)”* [36], the build will also consider how such concepts as trust and risk are of great importance when dealing with security: alleged technical-only decisions can have a decisive influence on the individual's trust toward the technical device or toward the organization that manages it and its associated services. Eventually (in the section after), we will draw on the previous section assumptions to establish some requirements for the design of privacy.

- **Security, privacy and the technical device<sup>1</sup>**
- *Understanding the links between security privacy and the technical device*

**Information security traditional core principles are confidentiality, integrity, availability and authenticity of the data being processed** [37]. Nevertheless, the concept can also be appreciated in a broader way. Dourish *et al* defined it as: *“The ability of users to express and rely upon a set of guarantees that a system may make, explicitly or implicitly,*

---

<sup>1</sup> *“Security and privacy are a “penultimate slide” problem for ubiquitous computing—the second to last slide in many conference presentation notes that there are security or privacy problems with the system that has been described, and that future work will address these issues. The “penultimate slide” syndrome indicates two things—first, that security and privacy issues are centrally implicated in the future success of ubiquitous computing, and, second, that they are currently poorly understood”.* [2] Dourish, P., et al., *Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem*. Personal and Ubiquitous Computing, 2004. 8(6): p. 391-401.

about its treatment of user data and other resources.” [2]. In the light of this definition, we understand that privacy violations can occur when a system is not secure and leaks personal data to unauthorized parties. Therefore, the concept of privacy<sup>1</sup> and the one of security appear to be strongly intertwined. However, **it would be misleading to reduce security as a mere technical translation of the privacy concept.**

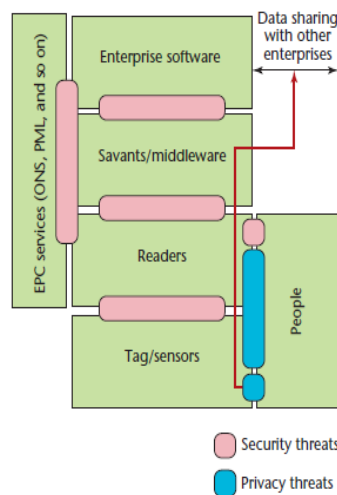


Figure 1. An abstract view of the EPC Network. The network defines standards for communication between tags and readers, and a set of EPC services, such as the Object Name Service (ONS) and Product Markup Language (PML), that enable scalable RFID networks. Pink boxes identify the location of threats to data security and blue boxes identify threats to personal privacy. The heavy red line calls out a special threat to personal privacy: the linking of personal identity to a set of unique tags. As personal identity moves up the stack and is stored and shared between enterprises, it becomes increasingly difficult to dissociate one's identity from the set of tags.

### Garkinkel *et al* [38]

Let us take the example of the Electronic Product code network to illustrate this assertion. As shown in this figure [38], security concerns and privacy ones are interrelated through data exchange processes. However, security's level of visibility<sup>2</sup> to the end user does not appear in this picture. Indeed, as for privacy paradigms<sup>3</sup>, we can say that the visibility of the security infrastructure design is determined by some security paradigms that define the user role in this “*mutual achievement of multiple parties*” [2] that is security. Therefore, the

<sup>1</sup> See the introductory section for the definitions of Privacy.

<sup>2</sup> By visibility, we mean the availability for a security system to be inspected, examined and acted upon.

<sup>3</sup> Bennett and Raab called *privacy paradigms* are “a set of assumptions based on more fundamental political ideas”. [6] Bennett, C.J. and C.D. Raab, *The Governance of Privacy: Policy instruments in global perspective*. 2003, Aldershot: Ashgate.

ability of the user to act upon the security features and to understand them is here the major factor that helps qualifying the security paradigm. This can be done by examining **the two paradigmatic poles between which security systems can circulate**:

- Security can be built as an impenetrable black box that let no opportunity for the user to manipulate the security parameters. Here the mechanics of the protecting technologies are totally hindered. **Security is here transparent to the user.**
- At the opposite, it can embody the involvement of the user to adjust security parameters to the context of use. In this case, the user has access to the functioning of the security infrastructure. It notably implies him/her to be able to understand how the system works. **Security is here visible to the user.**

What is at stake here is the management of borders' definition: **how far can we give the user the ability to understand and to act on security parameters to secure its privacy?** In other words, how involved would the user be in the management of what Altman [39] calls *Boundary regulation*? When it comes to privacy, "*Privacy management is not about setting rules and enforcing them; rather, it is the continual management of boundaries between different spheres of action and degrees of disclosure within those spheres. Boundaries move dynamically as the context changes. These boundaries reflect tensions between conflicting goals; boundaries occur at points of balance and resolution.*" [40]. Therefore, the designer working on security has to be aware of the dynamics of use the build system will inscribe<sup>1</sup> into the setting [42]. Some Human-Computer Interaction researchers have integrated this point so far that they consider **privacy as a central design issue**: "*We take privacy to be a personal notion shaped by culturally determined expectations and perceptions about one's environment. The social practices and policies that determine any rights an individual has to privacy interact with the technical and interface design aspects of the technology they use. Technology is not neutral when it comes to privacy. It can increase or reduce the extent to which people have control over personal data. Our concern is to ensure that privacy should be a central design issue in its own right.*" [8, our emphasis].

---

<sup>1</sup> "Like a film script, technical objects define a framework of action together with the actors and the space in which they are supposed to act." [41] Akrich, M., *The De-Description of Technical Objects*, in *Shaping Technology/Building Society*, W. Bijker and J. Law, Editors. 1992, The MIT Press: Cambridge London. p. 205-224.

Hence, CPM Manager like systems should be considered as **more than only disconnection technologies**<sup>1</sup>. This latter definition is not an improper one. It is only incomplete in that it fails to integrate the dynamics sides of security and privacy. It rules out the contextual and situational parts of privacy in reducing technologies to their technical aspects. In doing so, it does not inscribe security into the privacy management processes: the different spheres of action and degrees of disclosure are here silenced. Indeed, **CPM manager like systems, as any security systems, belong to the family of “privacy-aware ubiquitous computing systems, i.e., systems that take the social fabric of everyday life into account and try to prevent unintended personal border crossings”** [43, our emphasis].

It is now necessary to go further in defining whether the **CPM manager is a PET (Privacy Enhancing Technology)** or just a data-security technology: *“The term Privacy-Enhancing Technology (PETs) refers to technical and organizational concepts that aim at protecting personal identity. These concepts usually involve encryption in the form of e.g. digital signatures, blind signatures, or digital pseudonyms. PETs have to be set apart from data-security technologies. It is one of the merits of the discussion on PETs that the concept of data security has been reclarified as to its limitations with regard to privacy protection. Data-security measures seek to render data processing safe regardless of the legitimacy of processing. Data security is a necessary but not a sufficient condition for privacy protection. PETs, on the other hand, seek to eliminate the use of personal data altogether or to give direct control over revelation of personal information to the person concerned. PETs are therefore closer to the social goals of privacy protection.”* [36].

Indeed, the frontier between PETs and data-security technologies seems to be thin. However, it gives us exciting food for thought: the former put the individual at the centre of the security system whereas the latter is merely regardless of the content and the context of what is going on. As the COPRIM project is one that intends to give control to the user<sup>2</sup>, the

---

<sup>1</sup> “Disconnection technologies can be used to separate authentication from identification and to keep distinct multiple ‘identities’ - both digital and ‘real world’ identities”. [35] *Dilemmas of Privacy and Surveillance: Challenges of Technological Change*. 2007, The Royal Academy of Engineering: London.

<sup>2</sup> “The main goal of the COPRIM project is to propose relevant and viable solutions from the economical point of view, in order to give again the full control to the user and by that to maintain the confidence which he carries to these electronic objects.” (COPRIM Technical Annex).

**CPM manager should necessarily satisfy the criteria that both characterize PETs and Privacy-Aware Ubiquitous Systems.** Would the CPM manager fulfil these conditions, it would also be prone to the incorporation of PETs inherent limitations. Two of them are particularly interesting for our project:

- The **CPM manager is to be implemented in a larger system, e.g. NFC enhanced cell phone.** Therefore, Burkert's claim is determinative to the project: *"Having designed a particular PETs system does not, in itself, guarantee that this system will be used only for the particular purpose it was intended for; we may not be sufficiently aware of hidden information such a system carries with it; we cannot be reasonably sure or predict which other non-PET system are or will be available to provide "additional knowledge" that allows us to decipher anonymity, thus limiting the effect of the PET elements."* [36]. This means that the **opportunities of interaction between under-systems that compose the NFC-enhance setting need to be taken into account to assess the PET's efficiency.** Moreover, it also means that **these interactions and their effects cannot be predicted altogether.** This confirms what Mullender and other scholars say about protection mechanisms: *"they are often only secure in principle. They are seldom secure in practice"* [44], the necessity of *"stressing out the possibility of inadvertent intrusions into privacy"* [45] and the fact that *"systems must be not only secure, but usably and practically secure"* [2]. This is why *"[o]ne would have to ensure not only that individual PET systems were designed properly but also that their role in networks of PET and non-PET systems remained clearly identifiable."* [36].
- Criticizing the reductionist temptation that considers security to be a mere translation of privacy (*"privacy as anonymity, or in more advance settings privacy as a conscious choice between anonymity and identification, or in even more refined systems privacy as an opportunity to freely variegate grades of anonymity"*), Burkert [36] establishes a link between privacy, security and the consequences for designing PETs. **The involvement of users and their ability to act dynamically on the system are no more considered as simple options. They are prerequisites in the design of PET:** *"First, PET design itself must be opened to participatory elements. This implies that designing PETs and implementing them in social systems must involve those whom these enhancements are supposed to serve. Second, PET designs would have to contain a broader variety of switches or modules that would allow for easily manageable situative choices."*

Abiding by these two definitions<sup>1</sup> are de facto conditions an integrated security system whose aim is to address privacy concerns. In addition, it enables us to retain a substantially **more operational definition<sup>2</sup> of privacy** that fits the design concerns when considering

<sup>1</sup> Those of PETs and Privacy-aware Ubiquitous Computing Technologies.

<sup>2</sup> See the following section called *How to Trust a sociotechnical order*.



privacy. Privacy (management) can then be operated as the “*control of outflow of information that may be of strategic or aesthetic value to the person and control of inflow of information, including initiation of contact. It includes non-release to a third party of information yielded by one party unless with explicit consent*” [46, our emphasis].

So far, we have demonstrated the contextual, situational and dynamic nature of privacy. We have eventually showed that “*the social practices and policies that determine any rights an individual has to privacy interact with the technical and interface design aspects of the technology they use.*” [8]. However, we have not yet examined the mechanisms that make an individual chose to get involved within this sociotechnical order [47]. In the following section, we will address how the notion of trust structures this sociotechnical order.

#### ■ ***How to Trust a sociotechnical order***

The **paradox of technological development** has been highlighted by some researchers: “*the unobtrusiveness of such technology [Ubiquitous Computing] both **obscures and contributes** to its potential for supporting invasive applications, particularly as users may not even recognize when they are on line in such an environment. Designers must therefore consider carefully how services that capitalize on such powerful technology can be designed without compromising the privacy of their users*” [48, our emphasis]. Accordingly, communication technologies – whether they are connection, disconnection or processing ones – and their associated applications **contain in themselves a hazardous side**. In some case, like for PETs’ designing or implementation, this hazard is explicitly targeted: the aim is to transform it into a risk that can be handled and reduced. The notion of risk draws its difference from this of hazard in that it can be simulated, evaluated and compared. The formula “*Risk = likelihood of occurrence × seriousness if incident occurred*” is a well-known one whereas the notion of hazard remains independent of any probabilistic calculation. **Differentiating risk and hazard will then prove of great importance to our project when considering it in the light of trust.**

When dealing with relationships between technologies and privacy – through the cursor of security, it is hard to avoid trust to be a core notion as communication technologies are made to mediate relationships (between objects, between humans and between objects and humans). Indeed, “*relationships are ties based upon trust, where trust is not pre-given but worked upon, and where the work involved means a mutual process of self-disclosure*” [49].

This process of self-disclosure is in the balance of privacy management as demonstrated above. **This negotiation's core term is then trustworthiness.** Relationships between trust, privacy and a technical device are circular as Samajiriva demonstrates: *“In some contexts, a person will voluntarily yield highly personal information and will not consider that release, by itself, a diminution of privacy. In other contexts, the most mundane information will be guarded with great care. The same applies to the reception of information. Privacy is a precondition for trust- an attitude developed on the basis of situational or experiential factors. Trust affects privacy. A user's trust in the information practices of a system is likely to make possible consensual surveillance, which can enhance trust<sup>1</sup>.”* Thus, **trust at the same time causes and results in privacy.** However, having illustrated this dynamic, it does not give us a satisfactory definition of trust<sup>2</sup>.

Sociologist Anthony Giddens' definition of it proves to be a quite comprehensive and clarifying one: *“confidence in the reliability of a person or a system, regarding a given set of outcomes or events, where that confidence expresses faith in the probity or love of another, or in the correctness of abstract principles (technical knowledge)”* [49]. Three elements are to be identified in this definition in respect to the COPRIM project's main objectives:

- **Who or what is to be reliable?** The aim of the project is to give the individual confidence in using a NFC enhanced device. Therefore, the targeted system is the technical one. This does not mean that other factors should not be taken into account. It simply defines what dimensions of trust can be reasonably targeted in terms of security designing.
- **What are the given set of outcomes or events to be taken into account?** The situational, contextual and dynamic parts of privacy are to be remembered to answer this question. Tackling the privacy problem necessarily involves considering significant patterns of use of the technical artefact to be of great interest for the design.
- **Toward what is this faith oriented?** In our project, it is obvious that what Giddens calls *abstract principles (technical knowledge)* are central to the building of a

---

<sup>1</sup> Although it is not focused on technological problems, Luhmann's assertion confirms these circular relationships. In order to understand it this way, it is however necessary to include technologies as potential systems: *“A system – economic, legal, or political – requires trust as an input condition. Without trust it cannot stimulate supportive activities in situations of uncertainty or risk. At the same time the structural and operational properties of such a system may erode confidence and thereby undermine one of the essential conditions of trust”.* [50] Luhmann, N., *Trust: Making and Breaking of Cooperative Relations*. 1988, Oxford: Blackwell.

<sup>2</sup> We will not discuss here different theories of trust. Our only aim is to know to what extent they can seriously influence the design of the CPM Manager.

trustworthiness relationship. However, it also introduces the idea that trust can possibly be based on less rational concepts.

This being said, the links between this definition of trust on the one hand and the concepts of risk and danger on the other remain unobvious. To put a light on these relationships, we need to appeal to Luhmann's **differentiation between "trust" (la confiance décidée) and "confidence" (confiance assurée)** [51]:

- Confidence's definition: « *La confiance assurée, de même que la connaissance qui lui est nécessaire, se basent sur plusieurs éléments. Elle peut se fonder sur **la capacité d'imposer des sanctions** et sur le fait de savoir que le partenaire d'interaction sait aussi quelle sanction lui sera infligée s'il ne respecte pas les termes d'un accord. Les sanctions peuvent être formelles ou informelles, elles peuvent être étayées sur un réseau complexe d'obligations de parenté ou sur les dispositions de la loi concernant les contrats. Elles peuvent être immédiates ou intergénérationnelles, symboliques ou matérielles.* » (our emphasis).
- Trust's definition: « *Elle est ce dont nous avons besoin quand nous n'avons pas, ou ne pouvons pas avoir, une confiance assurée, en particulier quand nous ne pouvons pas prédire les comportements et leurs conséquences. La confiance décidée est ce dont nous avons besoin lorsque nous **sommes en interaction avec des étrangers**. Elle est ce qui est nécessaire quand nous ne pouvons pas connaître l'autre, i.e. quand nous ne sommes pas en mesure de lui attribuer un comportement ou de le prédire, parce que soit a) il n'existe aucun système au sein duquel des sanctions pourraient être imposées, soit b) on ne trouve aucun élément de familiarité ou de similitude permettant une telle attribution ou une telle prédiction.* » (our emphasis).

This distinction enables us:

- to understand to what extent the **COPRIM Project addresses Trust rather than Confidence**. The will to involve the user in the security system functioning seems to be very strong in the project. Therefore, the system includes a certain degree of freedom of action for the user. This is what Luhmann identifies in Trust: "***La confiance décidée n'est pas seulement un moyen de négocier le risque, elle implique également ce risque*** (et cela par définition, si elle est un moyen de négocier ce qui est inconnu). Le risque impliqué est précisément ce qui est inhérent à la liberté d'action d'autrui. Si toutes les actions étaient délimitées par des attentes de rôle et des définitions normatives, il n'y aurait pas de risque mais uniquement une confiance assurée [Trust] ou un manque de confiance." (our emphasis).
- to **take into account the different social representations of risk**. "*La distinction entre confiance assurée et confiance décidée dépend ainsi de la **perception et de l'attribution**. Si vous n'envisagez pas d'alternatives (vous quittez votre maison chaque matin sans vous armer !), vous êtes dans une situation de confiance assurée [confidence]. Si vous choisissez une action de préférence à d'autres, en dépit de la possibilité d'être déçu par l'action des autres, vous définissez la situation comme une situation de confiance décidée [trust]. Dans le premier cas, vous réagirez aux*

*déceptions par des attributions externes. Dans le second, vous aurez à considérer une attribution interne et éventuellement à regretter d'avoir choisi de faire confiance.”* (our emphasis). This is directly related to the first assertion.

The major consequence of these two remarks is that in case of a successful attack, the **attribution of responsibility** could vary a lot. It would depend on the individual perception of the situation:

- Does it result from a faulty privacy management from the individual? In that case, a risk has been taken by the individual and the **attributions of the attack have chances to be assumed by him/her**.
- Does it result from the inability of the device to be secure enough? In this case, the individual considers that **the system was faulty in doing bad privacy management**. Wrong choices have been made that did not include at any levels the individual.
- Does it result from a threatening environment? That case illustrates the links between danger and confidence. The danger exists without any alternatives to avoid it. **External attributions will explain the successful attack** for the individual.

Thus, it clearly appears that the attribution of responsibility in case of a faulty privacy management can extensively vary. It then **depends also on the degree of freedom the user can be entitled with its use of the CPM**. One way of not losing from our sight this plasticity of causal attribution in case of a successful attack is to consider how security perceptions structure the trustworthiness of the user toward a security system thanks to the mechanism of delegation brought into light by Dourish *et al* [2].

Studying the problems of security and information technologies, Dourish *et al* [2] have shown that security are differentially experienced by end-users. First of all, they distinguish three kinds of attitude toward security that are non exclusive:

- **Frustration** stresses out the barriers and drawbacks of some security systems. These appear to be obstructive for the use of the device. Talking about some interviewees, the authors state: *“They were more likely to talk of security in terms of its costs as well as its benefits, and frame technical security measures as ones that can interfere with the practical accomplishment of work.”*
- **Pragmatism**: *“Pragmatic users see security as a trade-off, one that must be continually struck as one balances immediate needs against potential dangers. For pragmatic users, then, systems need to be both flexible and translucent, so that these trade-offs can be made effectively.”*

- **Futility:** The users here do not focus on security as an essential protection mechanisms against privacy assaults. Rather, *“they talk repeatedly of security lying not so much in technology as in vigilance; the continual, active defence against new and evolving threats.”*

Integrating these attitudes puts our concerns toward privacy and new technologies in perspective. The user is then not only a part of security system as we have seen above. When using these systems, he/she interprets its role and at the same time redefines the system. Therefore, the efficiency of this system (or its disadvantages) can endure strong distortions in respect to the users’ perception of it. The authors find three explanations of these distortions that form the gap between theoretical security and effective secured as experienced by end users:

- Security can be rejected by end-users for not providing a comprehensive solution to their problems.
- A security system aiming at protecting against one specific threat can be mistakenly interpreted as providing solutions to other problems.
- The focus on barriers or “choke points” diverts attention from channels and their contents.

This notably explains how, in practice, security undergoes delegation mechanisms. *“Security is, to some extent, turned into someone else’s problem, or at least, external resources are marshaled to deal with the problem.”* Three forms of delegation are identified:

- **Delegation to technology:** this requires the individual to understand *“the vulnerabilities that these technologies prevented, and what the limitations of each was, and how to use them in combination to create secure solutions. In other words, it was an argument that was only available to those who could, in fact, turn a technically working security system into an individually workable solution.”*
- **Delegation to another individual:** the knowledge or skill of a knowledgeable person is here the important criterion.
- **Delegation to an organization** (e.g. work place) and institutions (for example, financial institutions).

So far, we have demonstrated that trust is a central issue for design privacy enhancing technologies. We have also proved that this concept – as for the privacy one and the security one – cannot be integrated in the design process as a monolithic one. It is constantly

negotiated during the interactions between the device and the end user, not only according to the reliability of the security system. It also depends on users' perception and practices of security. Therefore, we acknowledge that it is trickier to consider all these observations than designing a system that only abides by the law in terms of privacy. The issue is all the more delicate that *"little is known about how to create a trust-conducive environment based on interactive systems. Trust in abstract systems depends on the "access points" or interfaces of the systems."* [46]. The concluding section will stress out these essentials.

## ■ Some operational lessons for design

*"Privacy is not a force to be tamed or overcome, like gravity or distance. It is an ongoing, fluid, cooperative human process that must be addressed and readdressed in the design of every privacy-affecting system. Rather than solving it, designs can accommodate it. And the way to do so is to empower the end-user to intuitively understand and influence the conditions that create it."* Langheinrich [43].

Throughout this short introducing journey into the conceptual waters of Privacy, it appears clear to us that two major pitfalls are to be avoided when designers are involved in the protection of privacy.

In regards to the very contingent nature of the concept, it could be strongly harmful to infer the success of a system at a worldwide level because of its triumph in a given western country. However, announced differences between cultural patterns are to be seen as one possible level of privacy's contingency understanding because what privacy is, that is a discriminating act: culture vs. culture, organization vs. organization, individual vs. individuals, organization vs. individual, state vs. organization, individual vs. states, family vs. neighbourhood, colleagues vs. suppliers, husband vs. wives, children vs. teachers, by-passers vs. bus-users, and so forth... Add Thomas' theorem to this complex state of affairs<sup>1</sup> and the

---

<sup>1</sup> *"If men define situations as real, they are real in their consequences."* See *The child in America: Behavior problems and programs*. W.I. Thomas and D.S. Thomas. New York: Knopf, 1928: 571-572.

subsequent plasticity of what comes under privacy or not – the contextual and dynamic interpretation of one acting individual – and the concept reveals its all contingency. **Wisdom then demands that if privacy is to be addressed, it cannot be done without taking into account its inherent instability.**

On the other hand, it could be tantalizing to deny that plasticity by reducing the concept of privacy to more simplistic definitions. This is especially true when privacy concerns are to be implemented in design. Whereas it is of great importance to have at disposal more or less obdurate tools – as ideational as they could be, reducing privacy to security or to information privacy is a hazardous gamble. At the opposite, considering these latter as under layers of the wide-ranging concept of privacy proves to be very useful in defining the scope of concerns a project can afford to tackle in regards to its available resources. **Therefore, as privacy dimensions are numerous (social, technical, economic, cultural, practical, etc.), any project aiming at protecting it is condemned to be unable to wholly address it.**

Our point here in presenting these apparently cheerless warnings is not to draw the conclusion that it is not conceivable to incorporate privacy into the design of an artefact. We just wanted to show how complex and humble this task can be when the concept has been beforehand explored. The last part of this work is subsequently largely inspired by exemplary framework established by Bellotti and Sellen [8] for designing for privacy. We agree with [8, 52] that designing for privacy essentially means thinking about control and feedback of data: *“These two issues are fundamental to successful communication and collaboration amongst users as well as to maintaining privacy”*. Control is thus defined as *“Empowering people to stipulate what information they project and who can get hold of it.”* Feedback is defined as *“Informing people when and what information about them is being captured and to whom the information is being made available.”*

Although Bellotti and Sellen’s study [8] focuses on systems that involve audio, video and computer networking, their proposed framework reveals itself to fit any project that affect privacy and innovative communication settings. Consequently, the following requirements for the design of the CPM Manager are identical to those Bellotti and Sellen identified in their work. In their framework, the researchers distinguish four interdependent user and system behaviours:

- **Capture:** The nature of information that is picked up.

- **Construction:** The manipulation and future of information (encryption, process, storing).
- **Accessibility:** The availability of information and the means deployed to access it.
- **Purpose:** The immediate use of the information and the future use of it (explicit or not).

	Feedback About	Control Over
<b>Capture</b>	When and what information about me gets into the system.	When and when not to give out what information. I can enforce my own preferences for system behaviours with respect to each type of information I convey.
<b>Construction</b>	What happens to information about me once it gets inside the system.	What happens to information about me. I can set automatic default behaviours and permissions.
<b>Accessibility</b>	Which people and what software (e.g., daemons or servers) have access to information about me and what information they see or use.	Who and what has access to what information about me. I can set automatic default behaviours and permissions.
<b>Purposes</b>	What people want information about me for. Since this is outside of the system, it may only be possible to infer purpose from construction and access behaviours.	It is infeasible for me to have technical control over purposes. With appropriate feedback, however, I can exercise social control to restrict intrusion, unethical, and illegal usage.

**Figure 1.** A framework for designing for feedback and control in ubiquitous computing environments: Each cell contains a description of the ideal state of affairs with respect to feedback or control of each of four types of behaviour.

They consider capture to be the most important in regards to our project's goal: *“For those concerned about privacy, and the potential for subversion in particular, control over, and thus feedback about, capture is clearly the most important. Given appropriate feedback about what is being captured, users can orient themselves appropriately to the technology for collaboration or communication purposes and exercise appropriate control over their*



*behavior or what is captured in the knowledge of possible construction, access and purposes of information use.”*

From their experiences, and drawing on their framework, they then propose a set of criteria to evaluate the privacy enhanced implemented solution. These criteria are:

- *“Trustworthiness: Systems must be technically reliable and instill confidence in users. In order to satisfy this criterion, they must be understandable by their users. The consequences of actions must be confined to situations which can be apprehended in the context in which they take place and thus appropriately controlled.*
- *Appropriate timing: Feedback should be provided at a time when control is most likely to be required and effective.*
- *Perceptibility: Feedback should be noticeable.*
- *Unobtrusiveness: Feedback should not distract or annoy. It should also be selective and relevant and should not overload the recipient with information.*
- *Minimal intrusiveness: Feedback should not involve information which compromises the privacy of others.*
- *Fail-safety: In cases where users omit to take explicit action to protect their privacy, the system should minimise information capture, construction and access.*
- *Flexibility: What counts as private varies according to context and interpersonal relationships. Thus mechanisms of control over user and system behaviours may need to be tailorable to some extent by the individuals concerned.*
- *Low effort: Design solutions must be lightweight to use, requiring as few actions and as little effort on the part of the user as possible.*
- *Meaningfulness: Feedback and control must incorporate meaningful representations of information captured and meaningful actions to control it, not just raw data and unfamiliar actions. They should be sensitive to the context of data capture and also to the contexts in which information is presented and control exercised.*
- *Learnability: Proposed designs should not require a complex model of how the system works. They should exploit or be sensitive to natural, existing psychological and social mechanisms that allow people to perceive and control how they present themselves and their availability for potential interactions.*
- *Low cost: Naturally, we wish to keep costs of design solutions down. The first seven criteria are especially relevant to protection of privacy. The final four are more general design concerns. Some of these criteria have to be traded off against one another in the search for design solutions.” [8]*

## ■ Existing solutions

---

### ■ Countermeasures on the physical layer

#### ■ *The “Kill” Tag Approach*

This solution consists of creating a new command, the “kill” command that enables the destruction of the tag which then can never be re-activated. The deactivation can be implemented by a fuse on the power supply of the chip or on the antenna, or by erasing of the memory. This command could be used, e.g., after checkout at a store. This approach ultimately solves all the problems of privacy. But outside a supply chain, all the advantages of RFID disappear. Thus, together with the destruction of the tag, all future benefits of Ambient Intelligence become quite reduced: no more possibility to make fridges interact with food or washing-machines with clothes. Even the control of a part of the supply chain is removed: tracking of items for recycling or for after-sale services is not feasible anymore. With such an approach, RFID only remains a tool to improve logistics of manufacturers and distributors. The implementation of the “kill” command implies also the use of a basic cryptographic algorithm to avoid the destroying of all the tags in the shop by a hacker [Sa02], [Jue03].

#### ■ *Optical Reading*

To avoid skimming of contactless cards, a solution was developed and implemented into electronic passports. This is the association of an optical reading with the contactless reading of the device often linked with symmetric algorithms. Only the data optically read on a two dimensional barcode of the passport enables the access to the contactless chip. A main weakness of this countermeasure is that a barcode can easily be copied. As a consequence, a passport should not be opened and shown to anyone else but the authorities. This condition is difficult to ensure, for example, as everybody has to present a passport during check in at hotels.

#### ■ *The Faraday Cage*

Another basic solution is to confine our RFID tags in a wallet made of a metallic sheet or mesh. This wallet plays the part of a Faraday cage blocking the HF and UHF radio signals of readers. The efficiency is certain but this approach is inefficient for big tagged objects that cannot be placed easily in containers. Another problem is raised by the fact that the RFID tags

will soon be so small that we will not know where they are. As a consequence, it will be impossible to pack them.

- ***Active Jamming***

It is possible to create a device that emits signals in the same bands as RFID readers to jam their communications with RFID tags. This solution has already been aforementioned in the denial of service attack. A lot of denial of service attacks could be seen also as a more or less efficient countermeasure. This device should broadcast signals with higher amplitude than the different standards permit, and, as a consequence, it should be illegal.

- ***Noisy Tags***

To prevent from eavesdropping on the communication, C. Castelluccia and G. Avoine [Ca06] developed a solution named "noisy tag". A special tag shares a key with the reader to create a secure communication channel. Thus, the noisy tag emits some bits generated with this key known only by the reader during the reply of the tag to the reader. The noise created by the noisy tag should prevent from eavesdropping. Still, the communication can be understood by the reader since it is able to subtract the noise. This approach however, introduces some major drawbacks. First of all, it requires a key agreement that implies to change the ISO standards for communication. Secondly, the noise generated is digital (bits are sent), so it will be really unlikely that a spying probe close by sees the signal from the noisy tag and from the original tag with the same amplitude. Consequently, it will be always possible to see a difference that is enough to retrieve the message from the tag.

- ***The Blocker Tag***

The blocker tag [Jue03] is already well documented in the previous chapter, since it can be also seen as an attack tool. The main drawbacks of the blocker tag to protect the user are that it cannot be selective (it will blur all tags). Also, this is a passive device that requires to be powered by the reader to work.

- ***The RFID Guardian***

The RFID Guardian ([Rie106], [Rie206], [Rie105], [Rie205]) is also aforementioned in the denial of service attack. It enables a large panel of services to protect the user: secret key management, authentication, access control, monitoring of the RFID environment, creation of collisions. It does not have the main drawbacks of the blocker tag, since it can be active.

Nevertheless, the selectivity can only be realized with ALOHA type anti-collision protocols, and this is not a multi-standards solution.

- **Solutions on the protocol level**

- ***Distance bounding protocol (UVSQ)***

- **Introduction**

Distance-bounding protocols have been proposed by Brands and Chaum in 1993 in order to detect relay attacks, also known as mafia fraud.

Such a protocol measures the delays between the sending out of a challenge and the reception of the response.

Two types of attacks against such secure protocols are considered in the literature: **mafia fraud** or mafia attack [Des88] (or Mig-in-the-middle [And01]) and **terrorist fraud** [Des88]. In the mafia fraud attack, the attacker does not perform any cryptographic operations based on the security protocol, and only forwards the challenges and the responses between the honest prover and the honest verifier. While in the terrorist fraud attack the prover is not honest and he collaborates with the attacker.

- **Known Protocols**

- **Brands and Chaum [BC93].**

Brands and Chaum [BC93] are the pioneers of distance-bounding protocols, they have designed several protocols secure against mafia fraud. In their settings it is assumed that

the prover possesses a signature key-pair: a private key (for signature), and a public one (for verification).

## GHOST

This basic protocol prevents the mafia frauds, but the prover can still cheat by sending out the bits  $\beta_i$  before receiving  $\alpha_i$ . The authors proposed a modification which prevents the prover from sending the bits  $\beta_i$  before receiving  $\alpha_i$  :

## TAG

Another solution in [BC93] which prevents the prover to send out bits too soon is to use random delays in the rapid bits exchange phase. This approach has the advantage from

a practical point of view that it does not require the commitment scheme. The authors also have pointed out that their protocols are not secure against terrorist fraud.

- **Waters and Felten [WF03].**

Waters and Felten [WF03] have designed a proximity-proving protocol with the extension that it protects the privacy of the prover and that the measured latency is afterwards transmitted to a third party which can reveal the identity of the prover.

The following figure describes a part of the protocol related to the proximity control. It is assumed that the verifier has an asymmetric encryption key-pair and that the prover possesses a signature key-pair.

LEECH

This protocol is secure against mafia fraud but not against terrorist fraud, since after preparing the first message a dishonest prover can delegate the execution of the protocol to an attacker.

- **Sastry, Shankar and Wagner [SSW03].**

The simplest distance-bounding protocol is probably the one proposed by Sastry, Shankar and Wagner:

#### Contactless communication

The use of random nonce prevents the prover to respond in advance, however without any authentication this protocol is vulnerable to the mafia attack. The authors have proposed a modification in which the parties share a common secret key  $s$ :

#### Contactless communication

However, the time spend for computing the reply can be so large with respect to the travel time as to make it difficult to compute the distance except for relatively slow mediums like sound (for which Sastry et al. protocol is designed).

- **Hancke et Kuhn [HK05].**

Hancke and Kuhn proposed in [HK05] a modification to the challenge-response scheme which improves the overall efficiency of the distance-bounding protocol. In their protocol (described below) both parties share a common secret key  $s$ .

Wireless or wired link

- **Bussard and Bagga [BB05].**

Bussard and Bagga proposed in [BB05] the first (to our knowledge) protocol secure against terrorist fraud. Their protocol (described below) is public-key based and uses zero-knowledge techniques, i.e. it is assumed that the prover owns a private key  $x$  and the verifier has the corresponding public key  $y$ .



- **Attacks based on exploitation of hardware weaknesses**

Thus the idea of Bussard and Bagga is to force the prover to give away his private key if he wants to mount a terrorist attack, since the attacker should own both  $e$  and  $s$  and hence  $x$ . On the other hand, the proposed protocol seems not feasible because of the asymmetric techniques and especially the zero-knowledge protocol – both computationally demanding.

- **Reid *et al.* [RNTS07].**

Recently Reid et al. [RNTS07] tried to combine the efficiency of the Hancke and Kuhn [HK05] protocol with the idea of Bussard and Bagga [BB05] for preventing terrorist attacks. In their protocol (see below), it is assumed that both parties share a common secret key  $s$ .

1. The prover randomly  $\beta_i \in_R \{0, 1\}$  for  $i = 1, \dots, k$ , where  $k$  is determined by a chosen security parameter.
2. Analogously the verifier randomly generates  $\alpha_i \in_R \{0, 1\}$  for  $i = 1, \dots, k$ .
3. After this preparation a phase of  $k$  rapid bit exchanges starts.
  - The verifier starts its timer and sends  $\alpha_i$  to the prover.
  - The prover replies with  $\beta_i$ .
  - Upon receiving the bit the verifier stops its timer.
4. The prover concatenates the  $2k$  bits  $\alpha_i$  and  $\beta_i$ , signs the result and sends it to the verifier.
5. The verifier concatenates the used  $2k$  bits  $\alpha_i$  and  $\beta_i$ , and verifies the received signature.

Brands and Chaum (basic protocol)

Note that the knowledge of  $m$  and  $e$  is equivalent to revealing the shared secret  $s$ . The authors claim that this will prevent a terrorist attack, but since the key  $s$  is less valuable for the prover than his private key and since it is used only for distancebounding, a corrupt prover may still mount a terrorist attack against the verifier.

▪ **Capkun and Hubaux [CH06].**

Capkun and Hubaux [CH06] have proposed the following protocol (see below). It is assumed that both parties share a common secret key  $s$ .

1. The prover randomly generates  $m_i \in_R \{0, 1\}$  for  $i = 1, \dots, k$ , where  $k$  is determined by a chosen security parameter.
2. Analogously the verifier randomly generates  $\alpha_i \in_R \{0, 1\}$  for  $i = 1, \dots, k$ .
3. The prover commits to  $m_1 \dots m_k$  and sends this commitment to the verifier.
4. After this preparation a phase of  $k$  rapid bit exchanges starts.
  - The verifier starts its timer and sends  $\alpha_i$  to the prover.
  - The prover replies with  $\beta_i = \alpha_i \oplus m_i$ .
  - Upon receiving the bit, the verifier stops its timer.
5. The prover concatenates the  $2k$  bits  $\alpha_i$  and  $\beta_i$ , signs the result, and sends it to the verifier, with the opening commitment to  $m_1 \dots m_k$ .
6. The verifier concatenates the  $2k$  bits  $\alpha_i$  and  $\beta_i$ , and verifies the received signature. Next he verifies the commitment and checks whether  $\beta_i = \alpha_i \oplus m_i$  for  $i = 1, \dots, k$ .

## ▪ Discussion

Brands et Chaum

As it has been pointed out by Singelee and Preneel [SP05], all known protocols except Waters, Felten and Capkun, Hubaux are using the idea of Brands and Chaum to measure the proximity by a rapid bit exchange. In order to measure the round trip time with accuracy special hardware is required. Moreover most of the today used communication channels have a bandwidth much bigger than a bit. Another observation made in [SP05] is that any protocol secure against mafia attacks can be made secure against terrorist attacks when trusted hardware is used. The trusted hardware has the following properties: it is impossible to change the protocol that it has to perform and it is impossible to derive any value out of it. Thus it can only be used as a black-box.

## ▪ The MIFARE solution

MIFARE is a smart card technology developed by Phillips (now NXP technology). The first MIFARE cards were sent in 1994, they are based on the ISO14443-A standard with radio frequency at 13.56 MHz.

This contactless card technology has been sent and used worldwide for 14 years. More than 1 billion of smart card ICs has been sold and 7 millions of corresponding readers have also been developed. Products based on this technology are considered as belonging to the RFID (Radio Frequency Identification) technology.

For years MIFARE has been extensively used in many different applications: loyalty, payment system for public transport, building access, identification products, and other applications.

Many MIFARE cards categories exist:

- The MIFARE Classic, the most spread product, it contains a proprietary encryption algorithm named CRYPTO1 hard wired and an EEPROM memory. Access in readings and writings to the memory are protected by authentication methods using the CRYPTO1 algorithm. Memory can be 1K, 2K or 4K bytes.  
This card has been recently (2008) hacked and vulnerabilities have been published in articles and web sites.

Many security systems based on it are nowadays broken and fragilized.

We will discuss about it in a next paragraph.

- MIFARE PRO: it integrates the MIFARE Classic plus a triple DES algorithm whose security is strong.
- MIFARE PROX it integrates a Public Key Infrastructure,
- MIFARE DESFire with a microprocessor,
- MIFARE DESFire SAM: based on MIFARE DESFire but built as a secure access module.

Many worldwide companies have licensed the MIFARE technology and integrated it in their products: Infineon, Atmel, Renesas ...

We will focus in this presentation of MIFARE on the MIFARE Classic whose vulnerabilities have been recently published.

## ▪ ***Functional Description of MIFARE***

### ▪ **Some features detail**

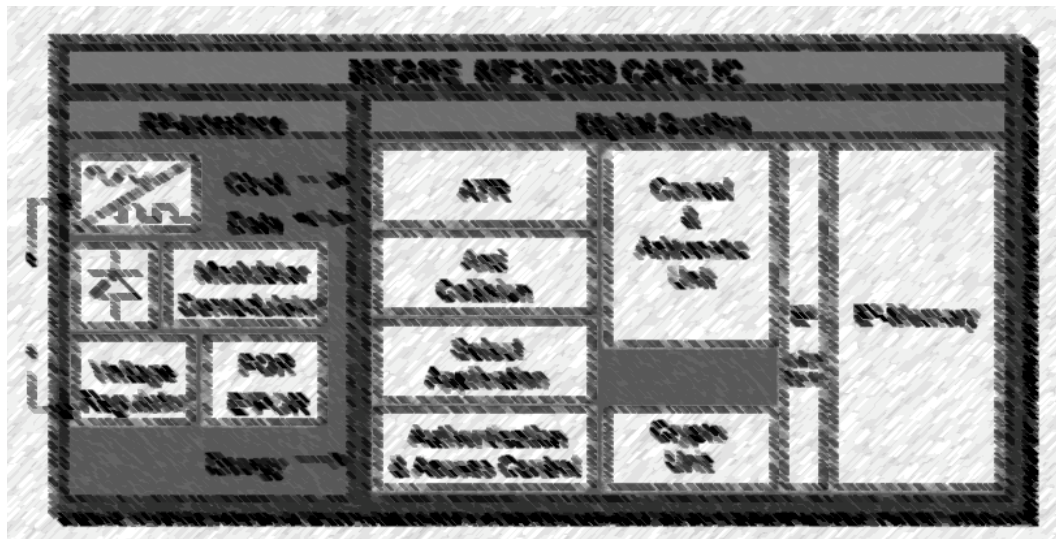
MIFARE is a multi-application smart card IC with many memory pages for the different applications. The functionalities for communication, computation generally done in smart cards by microprocessor are here done with hard wired logic. Dedicated design had been added for performance optimization and security.

The card can process with a distance from the reader up to 10cm in best cases; it depends from the power of the field emitted and from the size of the antenna connected to the device, cf. the following figure.



*MIFARE 1K Image*

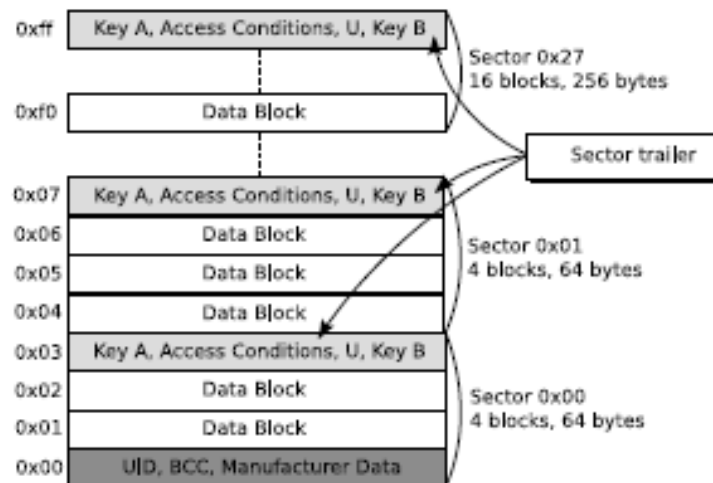
Anticollision is based on ISO1443-A protocol, the CSN (Card Serial Number) of each card is unique and used to select the cards emitting to the reader.



*MIFARE Block Description*

Data integrity checks are used for communication: Anticollision, 16-bit CRC per block, 16-bit parity per block, bit count checking, bit Coding to distinguish between '0' and '1', channel monitoring ...

The memory can be split in many sectors; each sector is subdivided in 16-bytes blocks. Each sector has its own secret file for a set of keys for systems using hierarchies.



Logical structure

## ■ **MIFARE Security**

To provide security authentication and encryption methods (ISO 9798-2) are used. They are based on a stream cipher algorithm coupled with a random number generator. The serial number and a 48-bit secret key are used for authentication.

1. The prover randomly generates two nonces  $s$  and  $r$  determined by a chosen security parameter.
  2. Next the prover signs its ID, then encrypts  $s$  with the security parameter to the verifier.
  3. The verifier decrypts the received message, extracts the signature.
  4. Next he generates a random nonce  $echo$  with length  $l$  and security parameter.
  5. After this preparation the phase of rapid exchanges starts:
    - The verifier starts its timer and sends  $(echo, t)$  to the prover.
    - The prover verifies that the first part of the received message is  $(echo, t)$  and replies with  $(reply, echo)$ .
    - Upon receiving the message back, the verifier checks the round-trip latency.
  6. The verifier checks that the received message is  $(reply, echo)$  and the second part is the nonce  $echo$ .
  7. The verifier sends a randomly generated nonce  $r_v$  to the prover.
  8. The prover returns it back to the verifier.
  9. The prover uses a pseudorandom function  $h$  (AES, or SHA-1) to compute the reply  $h(s; r)$  sent to the verifier.
- Sastry, Shankar et Wagner (modified)
- where  $k$  is a security parameter.
- The prover randomly generates a nonce  $r_p$  and sends it to the verifier.
- The verifier randomly generates a nonce  $r_v$  and sends it to the prover.
- Both parties use (one-way and collision resistant) function  $h$  to compute the reply  $h(s; r)$  sent to the verifier.
- The verifier randomly generates  $a_i$  for  $i = 1, \dots, k$ .
- The prover randomly generates  $a_i$  for  $i = 1, \dots, k$ .
- After this preparation a phase of  $k$  rapid bit exchanges starts.

The security of this protocol is based on the CRYPTO1 stream cipher and the quality of the pseudo random number generator PRNG1. Those two mechanisms have been secret for years, it was helpful for the security as the secret key used are only 48-bits.

But in 2007 [NOH08] those algorithms were reversed engineered by researchers. Their work has been published and it was the beginning of new attacks and publications on MIFARE, such as [DeK08].

We can now detail the algorithms hard wired in MIFARE cards.

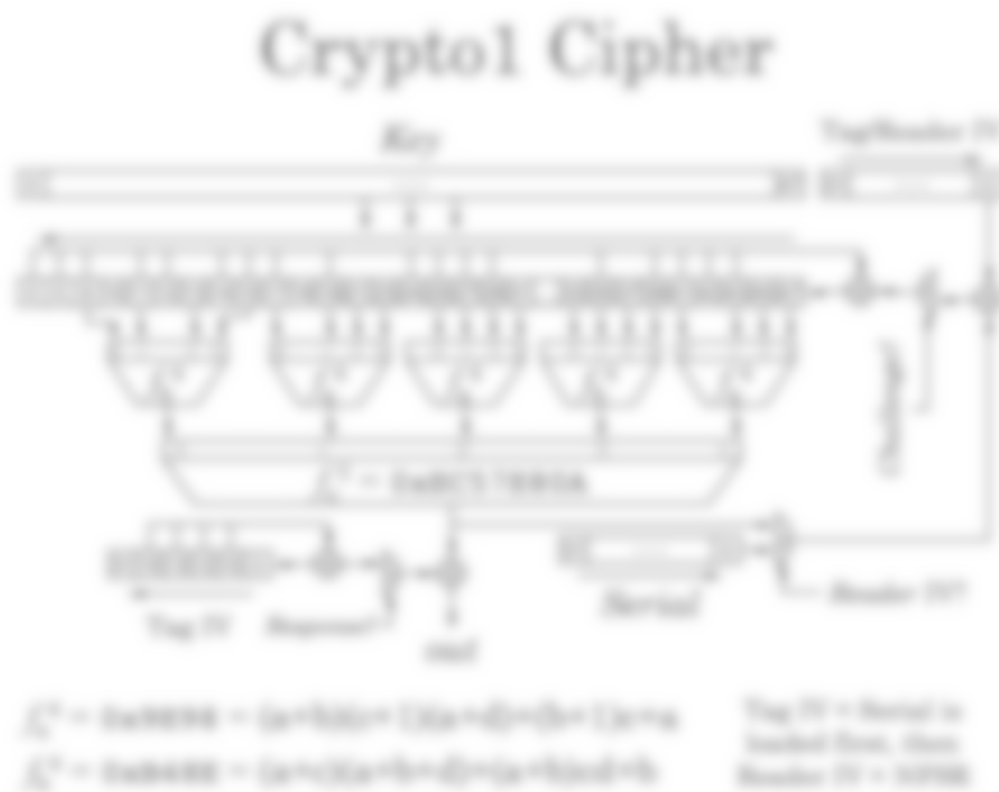
- **Pseudo Random Number Generator PRNG1**

It is a LFSR (Linear Feedback Shift Register) based on the polynomial  $X^{16}+X^{14}+X^{13}+X^{11}+1$ . It is initialized with a constant when the card is powered up by the reader.

- **CRYPTO1**

It is a 48-bit LFSR with generating polynomial  $X^{48}+X^{43}+X^{39}+X^{38}+X^{36}+X^{34}+X^{33}+X^{31}+X^{29}+X^{24}+X^{23}+X^{21}+X^{19}+X^{13}+X^9+X^7+X^6+X^5+1$ .

The output of the LFSR goes through a filter function  $f$  to give the encrypted result.



## ■ Weaknesses

1. PRNG1 has weaknesses, for instance with a frequency of 106kHz, it becomes cyclic with a periodicity of 0.6s, it is then used by researchers to know the random generated.
2. Knowing CRYPTO1, with the knowledge of two challenge/response data between a card and a reader, an exhaustive search on the key can be conducted as the key is only 48-bits.
3. In [DeK08] another and more efficient was conducted, with the method they explain, once precomputations have been done, the attack can be conducted in few minutes.

## ■ Conclusion

MIFARE security is nowadays broken, schemes based on MIFARE classic are nowadays very exposed to hacking and it should be replaced to prevent problems for the applications based on it.

## ■ Bibliography

---



- [1] Griesemer, J. and S. Star, *Institutional Ecology, Translations and Boundary Objects: Amateurs and Professionals in Berkeley's Museum of Vertebrate Zoology (1907-1939)*. Social Studies of Sciences, 1989. 19.
- [2] Dourish, P., et al., *Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem*. Personal and Ubiquitous Computing, 2004. 8(6): p. 391-401.
- [3] Demeulenaere, P., *Les difficultés de la caractérisation de la notion de vie privée d'un point de vue sociologique*, in *La protection de la vie privée dans la société d'information*, P. Tabatoni, Editor. 2002, PUF: Paris. p. 199-206.
- [4] de Singly, F., *Intimité conjugale et intimité personnelle. A la recherche d'un équilibre entre deux exigences dans les sociétés modernes avancées*. Sociologie et sociétés, 2003. 25(2): p. 79-96.
- [5] Ariès, P. and G. Duby, eds. *Histoire de la vie privée*. 1999, Points: Paris.
- [6] Bennett, C.J. and C.D. Raab, *The Governance of Privacy: Policy instruments in global perspective*. 2003, Aldershot: Ashgate.
- [7] Bennett, C.J., *Computers, Personal Data, and Theories of Technology: Comparative Approaches to Privacy Protection in the 1990s*. Science, Technology, & Human Values, 1991. 16(1): p. 51-69.
- [8] Bellotti, V. and A. Sellen. *Design for privacy in ubiquitous computing environments*. in *ECSCW'93: Proceedings of the third conference on European Conference on Computer-Supported Cooperative Work*. 1993: Kluwer Academic Publishers.
- [9] Miller, A., *The assault on privacy*. 1971, Ann Arbor: University of Michigan Press.
- [10] Westin, A.F., *Privacy and Freedom*. 1967, New York, NY: Atheneum.
- [11] Bennett, C.J., *Computers, Personal Data, and Theories of Technology: Comparative Approaches to Privacy Protection in the 1990s*. Science, Technology, & Human Values, 1991. 16: p. 51-69.
- [12] Sirey, B., *La notion de "privacy" au coeur des pratiques de consommation*, in *6ème Journées Normandes de Recherche sur la Consommation : Société et consommations*. 2007, Groupes ESC Rouen: Rouen.
- [13] Weiser, M., *The computer for the 21<sup>st</sup> century*. Sci. Am, 1991. 265(3): p. 94-104.
- [14] Weiser, M., *Some computer science issues in ubiquitous computing*. Commun ACM, 1993. 36(7): p. 74-83.

- [15] Bohn, J., et al., *Social, Economic and Ethical Implications of Ambient Intelligence and Ubiquitous Computing*. (2004), Zurich: Institute for Pervasive Computing.
- [16] Ackerman, M.S., *Privacy in pervasive environments: next generation labeling protocols*. Personal and Ubiquitous Computing, 2004. 8(6): p. 430-439.
- [17] Warren, S. and L. Brandeis, *The right to privacy*. Harvard Law Review, 1890. 4: p. 193-220.
- [18] Clarke, R., *Information Technology and Dataveillance*. Communications of The ACM, 1988. 31(5): p. 498-512.
- [19] Schoeman, F.D., *Philosophical dimensions of privacy: An anthology*. 1984, Cambridge: Cambridge University Press.
- [20] Harper, R., M. Lamming, and W. Newman, *Locating systems at Work: Implications for the Development of Active Badge Applications*. Interacting with computers, 1992. 3(4): p. 343-363.
- [21] Bates, A.P., *Privacy-a Useful Concept?* Social Forces, 1964. 42(4): p. 429-434.
- [22] Latour, B., *Where Are the Missing Masses? The Sociology of a Few Mundane Artifacts*, in *Shaping Technology/Building Society*, W. Bijker and J. Law, Editors. 1992, The MIT Press: Cambridge London. p. 226-258.
- [23] Latour, B., *Science in Action. How to follow scientists and engineers through society*. 1987, Cambridge: Harvard University Press.
- [24] Schwartz, B., *The Social Psychology of Privacy*. The American Journal of Sociology, 1968. 73(6): p. 741-752.
- [25] Stone, M.G. and M. Warner, *Politics, privacy and computers*. Political Quarterly, 1969. 40: p. 256-267.
- [26] Regan, P.M., *Public uses of private information: A comparison of personal information policies in the U.S and Britain*. 1981, Cornell University: Ithaca, NY.
- [27] Sieghart, P., *Privacy and computers*. 1976, London: Latimer.
- [28] Katz, J.E., *Telecommunications and computers: Whither privacy policy?* Society, 1987. 25: p. 81-86.
- [29] Coleman, J., *Foundations of Social Theory*. 1990, Cambridge and London: The Belknap Press of Harvard University Press.
- [30] Marx, G.T., *Murky Conceptual Waters: the Public and the Private*. Ethics and Information Technology, 2001. 3(3): p. 157-169.

- [31] Brin, D., *The Transparent Society*. 1998, Reading, MA: Perseus Books.
- [32] Sprenger, P. (1999) *Sun on Privacy: 'Get Over It'*. wired.com.
- [33] Cochrane, P., *Head to Head*. Sovereign Magazine, 2000: p. 56-57.
- [34] Phillips, D.J., *Cryptography, Secrets, and the Structuring of Trust*, in *Technology and Privacy : The New Landscape*, P.E. Agre and M. Rotenberg, Editors. 2001, The MIT Press: Cambridge. p. 243-276.
- [35] *Dilemmas of Privacy and Surveillance: Challenges of Technological Change*. 2007, The Royal Academy of Engineering: London.
- [36] Burkert, H., *Privacy-Enhancing Technologies: Typology, Critique, Vision*, in *Technology and Privacy: The New Landscape*, P.E. Agre and M. Rotenberg, Editors. 2001, The MIT Press: London. p. 125-142.
- [37] Aceituno, V., *On Information Security Paradigms*. ISSA Journal, 2005.
- [38] Garfinkel, S.L., A. Juels, and R. Pappu, *RFID Privacy : An Overview of Problems and Proposed Solutions*. IEEE Security and Privacy, 2005: p. 34-43.
- [39] Altman, I., *The Environment and Social Behavior: Privacy, Personal Space, Territory and Crowding*. 1975, Monterey, CA: Brooks/Cole Pub. Co., Inc.
- [40] Palen, L. and P. Dourish, *Unpacking "privacy" for a networked world*, in *Proceedings of the SIGCHI conference on Human factors in computing systems*. 2003, ACM: Ft. Lauderdale, Florida, USA.
- [41] Akrich, M., *The De-Description of Technical Objects*, in *Shaping Technology/Building Society*, W. Bijker and J. Law, Editors. 1992, The MIT Press: Cambridge London. p. 205-224.
- [42] Akrich, M. and B. Latour, *A Summary of a Convenient Vocabulary for the Semiotics of Human and Nonhuman Assemblies*, in *Shaping Technology/Building Society*, W. Bijker and J. Law, Editors. 1992, The MIT Press: Cambridge London. p. 259-264.
- [43] Langheinrich, M. *Privacy by Design -- Principles of Privacy-Aware Ubiquitous Systems*. in *Proceedings of the Third International Conference on Ubiquitous Computing (UbiComp 2001)*. 2001. Atlanta: Springer-Verlag.
- [44] Mullender, S., *Protection*, in *Distributed Systems*, S. Mullender, Editor. 1989: Addison Wesley.

- [45] Heath, C. and P. Luff. *Disembodied Conduct: Communication through Video in a Multimedia Office Environment*. in *ACM Conference on Human Factors in Computing Systems, CHI'91*. 1991. New Orleans, Louisiana.
- [46] Samarajiva, R., *Interactivity As Though Privacy Mattered*, in *Technology and Privacy: The New Landscape*, P.E. Agre and M. Rotenberg, Editors. 2001: The MIT Press. p. 277-310.
- [47] Law, J. and W. Bijker, *Postscript: Technology, Stability, and Social Theory*, in *Shaping Technology/ Building Society*, W. Bijker and J. Law, Editors. 1992, The MIT Press: Cambridge London. p. 290-308.
- [48] Bellotti, V., *Design for Privacy in Multimedia Computing and Communications Environments*, in *Technology and Privacy: The New Landscape*, P.E. Agre and M. Rotenberg, Editors. 2001, The MIT Press: Cambridge. p. 63-98.
- [49] Giddens, A., *The Consequences of Modernity*. 1990, Stanford: Stanford University Press.
- [50] Luhmann, N., *Trust: Making and Breaking of Cooperative Relations*. 1988, Oxford: Blackwell.
- [51] Seligman, A., *Complexité du rôle, risque et émergence de la confiance*. Réseaux, 2001.
- [52] Lederer, S., *Designing Disclosure: Interactive Personal Privacy at the Dawn of Ubiquitous Computing*, in *Computer Science Division*. 2003, University of California: Berkeley.
  
- [And01] R. Anderson, *Security Engineering: A Guide to building dependable distributed systems*, John Wiley and Sons, 2001.
  
- [BB05] L. Bussard, W. Bagga, *Distance-bounding proof of knowledge to avoid real-time attacks*, IFIP/SEC, 2005.
  
- [BC93] S. Brands, D. Chaum. *Distance-bounding Protocols*, EUROCRYPT'93, LNCS 765. 1993, pp. 344-359.

- [BH1] Black Hat/Defcon 2006: Hackers Go Back to Vegas article de TG Daily
  
- [BRE1] EP1183642 FR2792440: integrated circuit device which is secured against attacks resulting from controlled destruction of an additional layer
  
- [CC] Common Criteria – Supporting Document – Mandatory Technical Document  
Application of Attack Potential to SmartCards  
April 2008 – Version 2.5 – Ref CCDB 2008-04-001
  
- [Ca06] Castelluccia, C., Avoine, G.: Noisy Tags: A Pretty Good Key Exchange Protocol for RFID Tags. In: Proceedings of CARDIS 2006, pp. 289–299 (2006)
  
- [CH06] S. Capkun, L. Buttyan, J.-P. Hubaux, SECTOR: Secure Tracking of Node Encounters in Multi-Hop Wireless Networks, SASN 2003, pp. 21-32.
  
- [Des88]. Y. Desmedt, Major security problems with “unforgeable” (feige)- at- shamir proofs of identity and how to overcome them, SecuriCom, 1988.
  
- [Dif] [www.difrwear.com/](http://www.difrwear.com/)
  
- [DeK08] G. De Koning Gans, J.-H. Hoepman and F. D. Garcia, *A practical Attack on the MIFARE Classic*, CARDIS 2008.
  
- [eESC] Open SmartCard Infrastructure for Europe – Vol 6. Contactless Technology – White Paper on Requirements for the Interoperability of Contactless Cards  
eESC TB6 Contactless SmartCards March 2003
  
- [EPC] EPC Class-1 Generation 2 UHF RFID Conformance Requirements Specification

- [EUR1] Eurosmart: White paper RFID technology security concerns, understanding secure contactless device versus RFID, October 2007.
- [EUR2] Eurosmart: Security challenge for contactless solutions, e-Smart September 21<sup>st</sup> 2007
- [FIKE1] T. FINKE, H. KELTER, (BSI): RFID - eavesdropping of communication between a reader and a transponder in case of ISO14443 system, Bonn 2004
- [HA1] G. HANCKE, University of Cambridge: Eavesdropping Attacks on High-Frequency RFID Tokens; July 11 2008
- [HA2] G. HANCKE, University of Cambridge: a practical attack on ISO14443 proximity cards
- [Ha3] Gerhard P. Hancke and Markus G. Kuhn, an RFID distance bounding protocol, March 2005. IEEE SecureComm 2005.
- [Han05] Gerhard Hancke. A practical relay attack on ISO 14443 proximity cards, 2005. <http://www.cl.cam.ac.uk/~gh275/relay.pdf>
- [HK05] G. Hancke, M. Kuhn, An RFID Distance Bounding Protocol, IEEE SecureComm, 2005, pp. 67-73.
- [HO1] Junko HOSHIDA, Article EETimes: Tests reveal e-passport security flaw, August 30<sup>th</sup> 2004.
- [HR07] M. Hlavac, T.Rosa. A Note on the Relay Attacks on e-passports? The Case of Czech e-passports, 2007
- [INS] Inside Contactless Internal Documentation

- [ISO14443] ISO 14443 Identification cards - Contactless integrated circuit cards - Proximity cards
- [ISO15693] ISO 15693 Identification cards - Contactless integrated circuit cards - Vicinity cards
- [ISO18000] ISO 18000 RFID for item management
- [ITG1] ITG: from the legends to the laws of the physics January 2006
- [Jue03] A. Juels, R.L. Rivest, M. Szydlo : Selective blocking of RFID tags for consumer privacy. In *10<sup>th</sup> Annual ACM CCS 2003*, May 2003
- [KIWO1] Ilan KIRSCHENBAUM, Avishai WOOL, School of electrical Engineering, Tel Aviv University: How to build a Low-cost, extended-range RFID Skim, may 8<sup>th</sup> 2006
- [KFWO1] Zvir KFIR, Avishai WOOL, School of electrical Engineering, Tel Aviv University: Picking virtual pockets using relay attacks on contactless smartcard system, Sept 2005
- [KR1] Peter KRONIGER, ACG Identification Technologie (Germany): cartes 2005
- [KW05] Ziv K\_r and Avishai Wool. Picking virtual pockets using relay attacks on contactless smartcard systems. In *Proc. 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm)*, pages 47.58, Athens, Greece, September 2005. IEEE.
- [MO1] Bert MOORE, AIM Global: RFID Security: Getting serious, February 9<sup>th</sup> 2006
- [Mobi] [www.mobilecloak.com](http://www.mobilecloak.com)

- [NFC]            NFC Forum [www.nfc-forum.org/](http://www.nfc-forum.org/)
- [NOH08]       K. Nohl, D. Evans, Starbug and H. Plötz, *Reverse-Engineering a Cryptographic RFID Tag*, Usenix Security Symposium, July 2008.
- [NV07]           V. Vikov, M. Vauclair,    Yet Another Secure Distance-Bounding Protocol.
- [PIM1]           Pirate magazine February 6th 2007: RFID : pour le meilleur ou pour le pire? [www.acbm.com](http://www.acbm.com)
- [RI1]            Rikcha study: Security Aspects and Prospective Applications of RFID Systems; Federal Office for Information Security (BSI) 2004
- [Rie106]       M.R. Rieback, G.N. Gaydadjiev, B. Crispo, R.F.H. Hofman, A.S. Tanenbaum. "A Platform for RFID Security and Privacy Administration" *20th USENIX/SAGE Large Installation System Administration conference (LISA 2006)*, Washington DC, December 2006.
- [Rie206]       M.R. Rieback, Patrick N.D. Simpson, B. Crispo, A.S. Tanenbaum. "RFID Malware: Design Principles and Examples" *Pervasive and Mobile Computing (PMC) Journal*, vol. 2(4): 405-426, Elsevier, 2006.
- [Rie306]       M.R. Rieback, B. Crispo, A.S. Tanenbaum. "Is Your Cat Infected with a Computer Virus?" *Proc. 4th IEEE Intl. Conf. on Pervasive Computing and Communications. (PerCom 2006)*, Pisa, Italy, March 2006.
- [Rie105]       M.R. Rieback, B. Crispo, A.S. Tanenbaum. "RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management." *Proc. 10th*



*Australasian Conference on Information Security and Privacy. (ACISP 2005),*  
Brisbane, Australia, July 2005

- [Rie205] M.R. Rieback, B. Crispo, A.S. Tanenbaum. "Uniting Legislation with RFID Privacy-Enhancing Technologies." *Proc. 3rd Conference on Security and Protection of Information. (SPI 2005)*, Brno, Czech Republic, May 2005.
- [RNTS07] J. Reid, J. Neito, T. Tang, B. Senadji, Detecting Relay Attacks with Timing Based Protocols, ACM ASIACCS, 2007, pp. 204-213.
- [SA02] S. E. Sarma, S. A. Weis, and D.W. Engels. Radio-frequency identification systems. In Burton S. Kaliski Jr., C. etin Kaya Ko,c, and Christof Paar, editors, *CHES '02*, pages 454–469. Springer-Verlag, 2002. LNCS no. 2523.
- [SC1] Evan SCHUMAN: Report Blasts Holes In Contactless Card Security Claims October 29<sup>th</sup> 2006
- [SP05] D. Singelee, B. Preneel, Location Verification using Secure Distance Bounding Protocols, IEEE Computer Society, 2005, pp. 834-840.
- [SSW03] N. Sastry, U. Shankar, D. Wagner, Secure Verification of Location Claims, ACM Workshop on Wireless Security, 2003, pp. 48-61.
- [Ste] [id289.securedata.net/stewartstand.com/merchantmanager/index.php](http://id289.securedata.net/stewartstand.com/merchantmanager/index.php)
- [WF03] B. Waters, E. Felten, Secure, Private Proofs of Location, Princeton Computer Science TR-667-03, 2003.

## **Annexe 3.**

### **COPRIM Scenarios. Specifications.**



## COPRIM Scenarios : Specifications

<b>Projet ANR-07-TLCOM-04 - COPRIM</b>	
<b>Date:</b> 31.08.09	<b>Issue:</b> V 3.0

**Authors:**  
 CEA LETI: F. Vacherand, O. Savry  
 UPMF: J. Lavoley, E. Anjembe, F. Forest  
 UVSQ: L. Goubin, C. Delarabie  
 INSIDE CONTACTLESS: B. Felix, C. Malaterre, V. Verneuil

**CONFIDENTIAL**

### Restricted mailing list

Mailing list	Name	Partner
ANR	Frank Tarrier	
COPRIM Technical team	Benoit Felix Vincent Verneuil Olivier Lavoley Emmanuel Anjembe Fabrice Forest Louis Goubin Olivier Savry Francois Vacherand	Inside Contactless Inside Contactless UPMF UPMF UPMF UVSQ CEA-LETI CEA-LETI

The information contained in this document is the property of the contractors. It cannot be reproduced or transmitted to third without the authorization of the contractors.

1/39

### Diffusion restreinte

**Attention:** Ce document contient des matériaux confidentiels appartenant à des comités de normalisation en cours ou des matériaux sous copyright issus de groupes de réflexion. Ce document ne doit pas être diffusé en dehors de l'ANR et des partenaires du projet. Une version publique sera disponible sur le site web du projet.

### Restricted mailing list

**Warning:** This document includes confidential data from current standardization works or copyright information from private active working groups. No diffusion is allowed beyond the ANR staff and the project consortium. A public version will be available on the website of the project.

### Historical

Change record	Date	Issue
creation	01.02.09	v 1.0
scenario 1 description		v 1.1
		to v 1.5
session opening added	16.03.09	v 1.6
skimming / relay attacks division	23.03.09	v 1.7
new framework adopted (cf. COPIL #4)	29.04.09	v 2.0
scenarios 2, 3 and 4 completed	05.06.09	v 2.1
sociological analysis integrated	10.08.09	v 2.2
conclusion update	21.08.09	v 2.3
Final review	31.08.09	v 3.0

### Keywords

Payment, ticketing, smart poster, device pairing, peer to peer, RFID, NFC, contactless, privacy, eavesdropping, skimming, relay attack, man in the middle attack, denial of service, side channel attack, DFA

## Table of contents

<b>1</b>	<b>GLOSSARY .....</b>	<b>6</b>
<b>2</b>	<b>INTRODUCTION .....</b>	<b>7</b>
2.1	SCENARIOS ANALYSIS' METHOD .....	7
2.2	GLOBAL OVERVIEW.....	8
2.3	SCENARIOS GENERAL PRESENTATION.....	9
2.3.1	Payment.....	9
2.3.2	Transport ticketing.....	9
2.3.3	Smart poster (contactless token).....	9
2.3.4	Device pairing (peer to peer).....	9
<b>3</b>	<b>REGULATION AND PERCEPTION OF PRIVACY'S BORDERS.....</b>	<b>10</b>
<b>4</b>	<b>SCENARIOS DESCRIPTION.....</b>	<b>11</b>
4.1	PAYMENT.....	11
4.1.1	Detailed description.....	11
4.1.2	Analysis.....	17
4.2	TRANSPORT TICKETING.....	19
4.2.1	Detailed description.....	19
4.2.2	Analysis.....	20
4.3	SMART POSTER (CONTACTLESS TOKEN).....	27
4.3.1	Detailed description.....	27
4.3.2	Analysis.....	29
4.4	DEVICE PAIRING (PEER TO PEER).....	31
4.4.1	Detailed description.....	31
4.4.2	Analysis.....	33
<b>5</b>	<b>CONCLUSION .....</b>	<b>34</b>
5.1	ON THE SCENARIOS DESIGN AND DESCRIPTION .....	34
5.2	ANALYSIS SUMMARIZING PART.....	34
<b>6</b>	<b>APPENDIX .....</b>	<b>36</b>
6.1	SOCIOLOGIC TOOLS.....	36
6.1.1	Beiloff Grid.....	36
6.2	CRYPTOGRAPHIC PROTOCOLS AND ALGORITHMS .....	36
6.2.1	SDA (Static Data Authentication).....	36
6.2.2	DDA (Dynamic Data Authentication).....	36
6.2.3	RSA (Rivest Shamir Adleman).....	36
6.2.4	ECDSA (Elliptic Curve Digital Signature Algorithm).....	37
6.2.5	DES (Data Encryption Standard).....	38
6.2.6	AES (Advanced Encryption Standard).....	38

7	BIBLIOGRAPHY .....	39
---	--------------------	----

## 1 Glossary

AES	Advanced Encryption Standard
ATR	Answer To Reset
CPA	Correlation Power Analysis
CPM	Contactless Privacy Manager
DES	Data Encryption Standard
DFA	Differential Fault Analysis
DPA	Differential Power Analysis
DH	Diffie Hellman Key Exchange
DSA	Digital Signature Algorithm
ECC	Elliptic Curve Cryptosystem
ECDSA	Elliptic Curve Digital Signature Algorithm
EEPROM	Electrically Erasable Programmable Read Only Memory
ISO	International Organisation for Standardisation
IC	Integrated Circuit
MAC	Message Authentication Code
OS	Operating System
OTP	One Time Programmable memory
PA	Power Analysis
PIN	Personal Identification Number
RAM	Random Access Memory
RFA	Radio Frequency Analysis
ROM	Read Only Memory
RSA	Rabin Shamir Adleman public key cryptosystem
RSA CRT	RSA with the Chinese Remainder Theorem
SCA	Side Channel Analysis
SPA	Simple Power Analysis
URL	Uniform Resource Locator

COPRIM	31.08.09	Consortium COPRIM	V 3.0	5/39
Project	Date	Author	Version	page



## 2 Introduction

### 2.1 Scenarios analysis' method

Privacy is a social construction<sup>1</sup>. The concept's definition is characterized with contingency because it relies on manifold contextual factors: history, social and cultural states. Furthermore, the concept of privacy is to be understood as strongly dependent on subjectivity. Scenarios are then to be built and read by getting into the final users' shoes. Therefore, use situations are analyzed from the user's points of views. However, as this work aims to produce indicators relevant to the CPM's specifications, the context of use is here strictly restricted to the transaction process.

Drawing from our analyses, we will be able to establish a system of hypotheses that will help evaluate what poses a threat to privacy protection. Doing this, we will evenly assess the dual concepts of confidence/trust<sup>2</sup> which are pivotal in this project. Our main objective is then to give insights to the role of design in privacy management : the available technical alternatives for each use case are not only distinguishable according to the control/feedback given to the user, they also endorse different philosophy of privacy management.

The first step of the analysis is distributed across each correspondent use case. For each of them, we show how visible<sup>3</sup> the CPM activity is to the user by examining the level of control and that of feedback s/he gets on it. This analysis is largely inspired by the grid established by Bellotti (Bellotti, 2001). Directly related to the previous step, we then draw assumptions about the type of confidence (trust/confidence) which could be dominant depending on the technical option taken into account. Here, the goal is to gain view on the possible ways for the user to delegate security management to different entities (Dourish, Grinter, Delgado & Joseph, 2004). Therefore, even though each analysis is

<sup>1</sup> Privacy (management) can then be operated as the "control of outflow of information that may be of strategic or aesthetic value to the person and control of inflow of information, including initiation of contact. It includes non-release to a third party of information yielded by one party unless with explicit consent" (Samara)va, 2001)

<sup>2</sup> Luhmann's differentiation between "trust" (la confiance dévolue) and "confidence" (confiance assurée) (Luhmann, 2001) :

- Confidence's definition: « La confiance assurée, de même que la connaissance qui lui est nécessaire, se basent sur plusieurs éléments. Elle peut se fonder sur la capacité d'imposer des sanctions et sur le fait de savoir que le partenaire d'interaction sait aussi quelle sanction lui sera infligée s'il ne respecte pas les termes d'un accord. Les sanctions peuvent être formelles ou informelles, elles peuvent être étayées sur un réseau complexe d'obligations de parenté ou sur les dispositions de la loi concernant les contrats. Elles peuvent être immédiates ou intergénérationnelles, symboliques ou matérielles. » (our emphasis).
- Trust's definition: « Elle est ce dont nous avons besoin quand nous n'avons pas, ou ne pouvons pas avoir, une confiance assurée, en particulier quand nous ne pouvons pas prédire les comportements et leurs conséquences. La confiance dévolue est ce dont nous avons besoin lorsque nous sommes en interaction avec des étrangers. Elle est ce qui est nécessaire quand nous ne pouvons pas connaître l'autre, i.e. quand nous ne sommes pas en mesure de lui attribuer un comportement ou de le prédire, parce que soit a) il n'existe aucun système au sein duquel des sanctions pourraient être imposées, soit b) on ne trouve aucun élément de familiarité ou de similitude permettant une telle attribution ou une telle prédiction. » (our emphasis). (See State of the Art for more details)

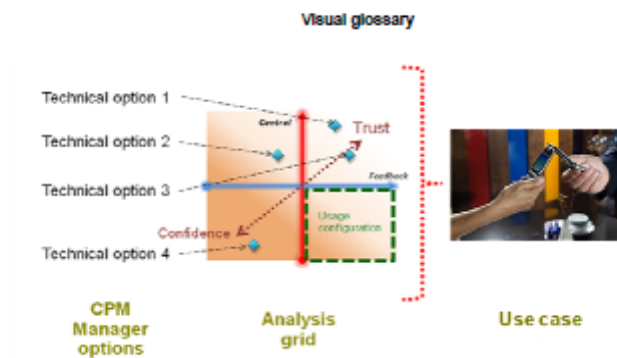
<sup>3</sup> Security can be built as an impenetrable black box that let no opportunity for the user to manipulate the security parameters. Here the mechanics of the protecting technologies are totally hindered. Security is here transparent to the user. At the opposite, it can embody the involvement of the user to adjust security parameters to the context of use. In this case, the user has access to the functioning of the security infrastructure. It notably implies him/her to be able to understand how the system works. Security is here visible to the user. (cf. state of the art)

COPRIM	31.08.09	Consortium COPRIM	V 3.0	7/39
Project	Date	Author	Version	page

case-related, a conclusive paragraph sums up the array of trends and questions that arise from all of the analysis.

The second summarizing part of this report sheds light on the role of design's issue by linking technical options to use configurations<sup>4</sup> in order to get a whole picture of the use cases. In so doing, we try to answer the question of design intervention in building privacy management in the COPRIM project.

In a third exploratory part, we extrapolate from the previous restricted analyses on the borders (Marx, 2001) of privacy jeopardized during the entire scenario.



## 2.2 Global overview

After having reviewed each use case according to the implications of their respective technical options in terms of control and feedback offered to the user, we have found two major trends that can :

- On the one hand, **user-centered design**<sup>5</sup>: when the user is given a great amount of control and feedback, we also conclude that this gives him/her insights of the risk at stake during the communication process. "Would the user want to know them?", "would the user like to manage (all of) them?" are some questions that follow from this observation.

<sup>4</sup> We call use configurations each quadrant of the analysis grid upon which technical options are projected.

<sup>5</sup> According to Donald Norman, user-centered design is "a philosophy based on the needs and interests of the user, with an emphasis on making products usable and understandable" Norman, D. The Design of Everyday Things. Basic Books, New York, (2002), p. 188

COPRIM	31.08.09	Consortium COPRIM	V 3.0	8/39
Project	Date	Author	Version	page

- On the other hand, Ubiquitous computing<sup>6</sup>: A lower level of control and feedback provoke here the risk here is that the device is not soft enough to meet changing users' expectations. Furthermore, it obliged us to consider other criterion than feedback and control to (socially) differentiate the options.

### 2.3 Scenarios general presentation

Four main scenarios have been set up to drive the works in the COPRIM project. They will be detailed in the next chapters.

#### 2.3.1 Payment

Every morning, Julie takes the bus to go to work. Thus, she needs to buy bus tickets. She could buy paper tickets but she prefers not to charge her wallet and to use her telephone NFC. Indeed, her NFC phone contains an application of classic banking payment and an application of transport which manages the electronic ticketing.

#### 2.3.2 Transport ticketing

Julie gets in the bus and validates the electronic ticket she has just bought. Other people have annual subscription held in their phone NFC transport application. During the run passengers tickets are checked by the company control staff.

#### 2.3.3 Smart poster (contactless token)

Today, Julie takes the bus with Yves, her grandfather. During the run, Julie points out an e-poster about a concert she's interested in. Yves suggests buying her a seat with his own NFC phone, she accepts.

#### 2.3.4 Device pairing (peer to peer)

Yves uploads the e-ticket he has just bought from his NFC phone to Julie's one. The Bluetooth file exchange is preceded by a NFC Bluetooth pairing.

<sup>6</sup> "Ubiquitous Computing (UbiComp) and/or Ambient Intelligence (AmI) refer to a vision of the future information society where humans will be surrounded by intelligent interfaces supported by computing and networking technology that is everywhere, embedded in everyday objects such as furniture, clothes, vehicles, roads and smart materials. It is a vision where computing capabilities are connected, everywhere, always on, enabling people and devices to interact with each other and with the environment. Computer devices are becoming increasingly small and cheap, interconnected and easy to use in order for them to find application in all aspects of our everyday lives. Computing capabilities will therefore not only be available in computing devices but also in everyday objects. These devices will be able to sense, think and communicate." In Puri, Yves. (2003). A social and technological view of Ambient Intelligence in Everyday Life (Technical Report EUR 20975 EN): Institute for Prospective Technological Studies, Directorate General Joint Research Centre, European Commission.

COPRIM	31.08.09	Consortium COPRIM	V 3.0	9/39
Project	Date	Author	Version	page

### 3 Regulation and perception of privacy's borders

If the presented use cases were exploited to help specifying the CPM, their writings will need a greater attention when they would serve as visual/textual aids during the acceptability tests. Our main hypothesis is that the socially differentiated perception of privacy's borders is a key variable of acceptability. Indeed, as securing the NFC communications does not prevent all privacy related threats linked to NFC use (cf. state of the art), we think that integrating prematurely the borders variable to the analysis would have been harmful at this stage of the project. It would have brought upon a mass of hypothesis inessential to the type of information required for specifying the CPM.

However, this work will be of great importance when confronting the project's production to the users' appreciation. It will enable evaluating the relevance of our hypothesis and that of users' perception of privacy in given use situations, of the secure ecosystem offered by the technical and social infrastructure, and of course of the CPM's role into that architecture.

The following grid (Manx, 2001) is thus actually incomplete but offers insights to the possible ways of padding the future writings of the scenario by taking into account more contextual hypotheses:

Sort of « borders »	Hypothesis examples
<b>Natural borders</b> Physical limitations of observations, such as walls and doors, clothing, darkness, but also sealed letters, telephone calls. Even facial expressions can form a natural border against the true feelings of a person.	The distance separating Julie from the machine, her cell phone location, night/day...
<b>Social borders</b> Expectations about confidentiality for members of certain social roles, such as family members, doctors or lawyers. This also includes expectations that your colleagues will not read personal fax messages addressed to you, or material that you left lying around the photocopy machine.	Julie is alone. The other human characters do not belong to her acquaintances. Other non human actants can be taken into account: CCTV...
<b>Spatial or temporal borders</b> The usual expectations of people that parts of their life, both in time and social space, can remain separated from each other. This would include a wild student time that should not interfere with today's life as a father of four, or different social groups, such as your work colleagues and lovers in your favourite bar.	
<b>Borders due to ephemeral or transitory effects</b> This describes what is best known as a "fleeting moment," an unreflected utterance or action that we hope gets forgotten soon, or old pictures and letters that we put out in our trash. Seeing audio or video recordings of such events later, or observing someone sifting through our trash, will violate our expectations of being able to have information simply pass away unnoticed or forgotten.	Informations displayed on her phone (photos, phone number), PIN Code...

COPRIM	31.08.09	Consortium COPRIM	V 3.0	10/39
Project	Date	Author	Version	page

## 4 Scenarios description

### 4.1 Payment

#### 4.1.1 Detailed description

To buy her electronic tickets, Julie uses a vending machine: she selects on the screen the number of tickets she wants to buy, and then she passes her NFC phone in front of the machine to pay her tickets.

This transaction can be made of various manners. Here are three possible procedures.

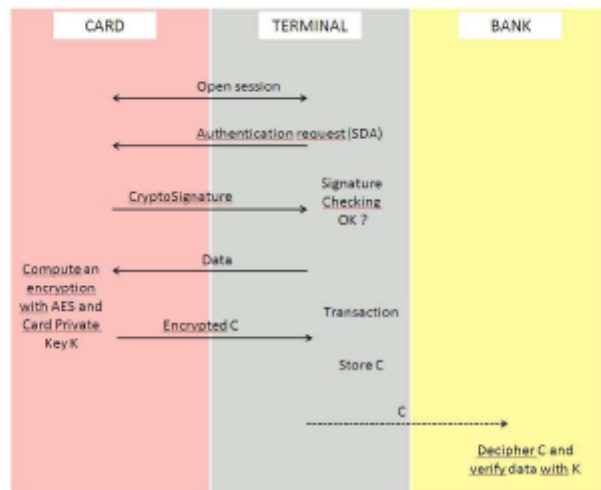
In the three cases, the card authentication is realized by using a cryptographic signature (called "CryptoSignature" in the following schemes). This signature may be static (SDA) or dynamic (DDA) and can be obtained with the RSA signature algorithm or the ECDSA algorithm. For more details, see the Appendix.

##### 4.1.1.1 Case 1: Offline, SDA/RSA, Encryption

Here, the card is the NFC phone containing a payment application.

The protocol used here for communication between the NFC and the reader is ISO/IEC 14443 Type B.

(In case where the payment application is embedded into a smart card connected to the NFC device, we consider the communication between the card and the NFC is done through the S2C "SigIn-SigOut-Connection" interface).



COPRIM	31.08.09	Consortium COPRIM	V 3.0	11/39
Project	Date	Author	Version	page

First of all, the terminal sends an authentication request (SDA). The NFC phone answers it by sending its signature SDA (see Appendix) and the terminal checks it.

Next, the terminal sends information to the phone (authorized amount, effective amount of the transaction ...). The card uses this data and its owner data to compute an encryption:

The algorithm used for computing the cryptogram corresponds to a CBC MAC with AES CBC with IV=0.

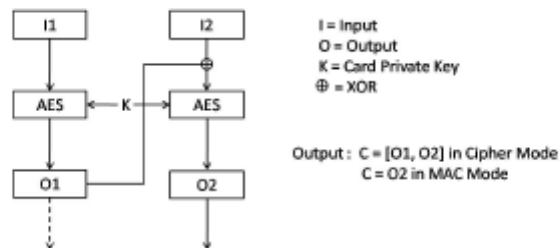
Input is 31-byte long and padded to 32 bytes:

Data provided by the Terminal:

- AA : Authorized Amount (6 bytes)
- EA : Effective Amount (6 bytes)
- TCC : Terminal Country Code (1 byte)
- TD : Transaction Date (3 bytes)
- TT : Transaction Type (1 byte)
- TC : Transaction Code (2 bytes)
- RND : Random Number (4 bytes)

Data provided by the Card:

- OC : Operation Counter (3 bytes)
- CDC : Card Data Check (4 bytes)
- CCC : Card Country Code (1 byte)
- Zero byte for padding (1 byte)



Computation:

- I1 = [AA|EA|TCC|TD]
- I2 = [TT|TC|RND|OC|CDC|CCC|00]
- O1 = AES(K)[I1]
- O2 = AES(K)[O1 ⊕ I2]

COPRIM	31.08.09	Consortium COPRIM	V 3.0	12/39
Project	Date	Author	Version	page



## Output is C = 02

The card sends C to the terminal and later (usually at the close of day), the vending machine will send C to the bank, and we say that the transaction is offline.

## Threats:

- **Eavesdropping:** NFC offers no protection against eavesdropping. An attacker can of course use an antenna to also receive the transmitted data. In practice a malicious person would have to keep a longer distance in order not to get noticed. The short range between Initiator and target for a successful communication is no significant problem, since attackers are not bound by the same transmission limits.

Here, an attacker can obtain the SDA signature of Julie's payment chip.

After, he will be able to produce a fake card using the SDA signature of Julie's card.

Making a fake card is easy today. Indeed anybody can buy a blank card and program it in C, Dephi, and Java ... (cf. MISC December 2008).

Such a fake card which contains as SDA value (static authentication) the one of Julie would be useful and could operate a fake transaction only in offline transaction.

In online transaction mode it would not be useful to have SDA Julie value.

- **Skimming:** This attack is based on a specific weakness of the contactless smartcards that is the possibility to activate the device without the consent of the user. Thus the device could get involved in an unwanted transaction or an attacker could also interact with it in order to obtain some (private) information.
- **Relay Attacks:** A relay attack is a particular case of skimming. Such an attack involves two different devices which we call the ghost and the leech and as a consequence two attackers. The ghost is a device which takes a card to the reader, and the leech is a device which takes a reader to the card. The main idea is to create a bidirectional communication between the genuine reader and the victim card passing through the leech and the ghost. To mount such an attack, one could place a leech device close to the victim (Julie) smartcard and then another could present the ghost to the reader at payment time.
- **RFA:** with contact cards, an attacker has to tamper with the terminal to collect the card consumption before performing a Side Channel Attack based on consumption analysis. Therefore a power analysis attack on a contact card need either to be done by a malicious merchant or by having stolen the card of the user to hack it quietly at home. With contactless card and NFC technology, data circulates in the air. So, from a distance (up to about 10 meters) an attacker can get access to the RF signal, obtain data transmitted and measure power consumed by the devices. Thus, it would be possible to perform such an attack by using an antenna. In attacking the computation of the cipher C, for instance by Radio Frequency Power Analysis, the attacker could retrieve K, the card's private key. Depending on the kind of attack, either he can realize a simple analysis and then a single execution is necessary, or he needs to obtain at least 30 to 100 messages for differential attacks. It will depend on the chip and on the security of the implementation. It is then not so easy to mount the attack but must be taken into account for any security analysis.

If he obtained the SDA signature by eavesdropping and if he has the card's private key, he will be able to make a clone of Julie's card which could work even in online transaction mode and then not be detected by the bank.

## Solutions:

- **Eavesdropping:** Establishing a secure channel between two NFC devices is clearly the best approach to protect against eavesdropping and any kind of data modification attack.

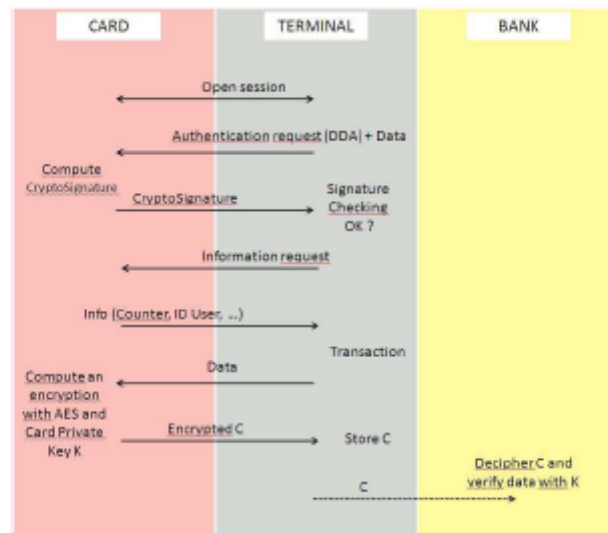
COPRIM	31.08.09	Consortium COPRIM	V 3.0	13/39
Project	Date	Author	Version	page

A standard key agreement protocol like Diffie-Hellman based on Integer Discrete Logarithm Problem or on Elliptic Curves Discrete Logarithm Problem could be applied to establish a shared secret between two devices.

The shared secret can then be used as a symmetric key (or to derive a symmetric key) in a 3DES or an AES which is then used for the secure channel providing confidentiality, integrity, and authenticity of the transmitted data.

- Skimming: To avoid skimming, we can introduce a user validation process (payment function activation or PIN validation).
- Relay attacks: To avoid relay attacks, we can also use a user validation process. When an intervention of the user is not desirable (for a (quick) ticket validation in transports for example), a specific protocol secure against relay attacks (distance-bounding protocol) can be used.
- RFA: To resist against Side Channel Analysis Attack, it is necessary to protect algorithms implementations as in classical contact secure elements (e.g. secure smart cards).

#### 4.1.1.2 Case 2: Offline, DDA/ECDSA, GetInfo, Encryption



First of all, the terminal sends an authentication request (DDA) with some data. The NFC phone computes a DDA signature (see Appendix) and the data provided by the terminal and answers by sending its signature.

COPRIM	31.08.09	Consortium COPRIM	V 3.0	14/39
Project	Date	Author	Version	page



Then, the terminal asks the card for some information. The card answers by sending requested data (transaction counter, Julie's identity ...)

Next, the terminal sends information to the phone (authorized amount, effective amount of the transaction ...). The card uses this data and its owner private key and data to compute an encryption C (in the same way as in the first case).

The card sends C to the terminal and later (usually at the close of day), the vending machine will send C to the bank (the transaction is offline).

#### Threats:

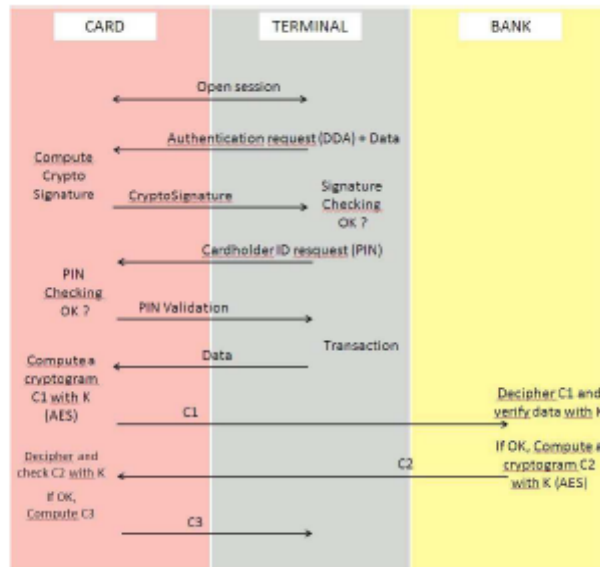
- **Skimming:** there is neither PIN verification nor validation processed by the user. Therefore, skimming is possible (see case 1).
- **Relay Attacks:** relay attacks are possible since no specific algorithm is used (see case 1).
- **Eavesdropping:** Some secret and private information about Julie are transmitted to the terminal, so the privacy is threatened.
- **RFA:** (see case 1) In attacking the computation of the signature, the attacker can retrieve the card's private key used in ECDSA. Moreover in attacking the computation of the cipher C, the attacker can retrieve K, the card's private key used in AES. If he obtained the card's private key for ECDSA signature and the card's private key for AES, he will be able to make a clone of Julie's card.

#### Solutions:

- **Skimming:** to avoid skimming, we can introduce a user validation process (see case 1).
- **Relay attacks:** to avoid relay attacks, we can use a distance-bounding protocol (see case 1).
- **Eavesdropping:** the best protection against eavesdropping is a secure channel between the terminal and the card (see Case 1).
- **RFA:** To resist against Side Channel Analysis Attack, it is necessary to protect algorithms implementations.

COPRIM	31.08.09	Consortium COPRIM	V 3.0	15/39
Project	Date	Author	Version	page

## 4.1.1.3 Case 3: Online, DDA/ECDSA, PIN, Encryption



First of all, the terminal sends an authentication request (DDA) with some data. The NFC phone computes a DDA signature (see Appendix) and the data provided by the terminal and answers by sending its signature.

Then, the terminal asks to Julie (the cardholder or the phoneholder) to prove her identity thanks to the PIN code. Julie types her PIN code on the keyboard of the vending machine (or of the phone, less probable) and the phone confirms (or not) the cardholder's identity to the vending machine.

Next, the terminal sends some information to the phone (authorized amount, effective amount of the transaction ...). The card uses this data and its owner data to compute an encryption C1. Here, the transaction is online so the cipher C1 differs from C: the algorithm used for computing the cryptogram is an AES CBC with IV=0. The computation is the same but the output is: C1 = [O1, O2].

The card sends C1 to the bank going through the terminal. The bank which knows card's private key deciphers C1 and checks data. If the bank validates the transaction, it sends a cipher C2 (encrypted with card's private key) to the card going through the terminal.

Finally, the card deciphers C2 with its private key then computes C3 and sends it to the terminal.

COPRIM	31.08.09	Consortium COPRIM	V 3.0	16/39
Project	Date	Author	Version	page

## Threats:

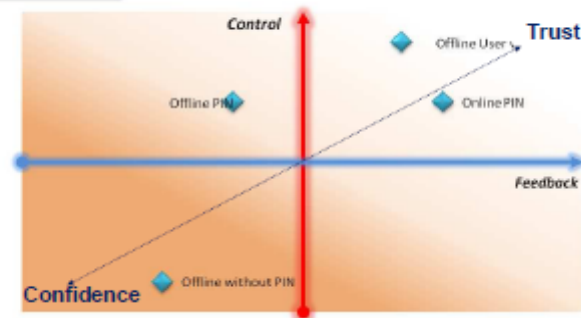
- Relay attacks: (see case 1)
- RFA: (see case 1) In attacking the computation of the signature, the attacker can retrieve the card's private key used in ECDSA. Moreover in attacking the computation of the cipher C, the attacker can retrieve K, the card's private key used in AES. If he obtained the card's private key for ECDSA signature and the card's private key for AES, he will be able to make a clone of Julie's card.

## Solutions:

- Relay attacks: distance-bounding protocols (see case 1)
- RFA: To resist against Side Channel Analysis Attack, it is necessary to protect algorithms implementations.

4.1.2 Analysis

## Payment cases



COPRIM	31.08.09	Consortium COPRIM	V 3.0	17/39
Project	Date	Author	Version	page

	Delegation of responsibility for security	Prevailing type of Confidence	Protection failure offloading process
Online PIN	<u>technology, individual, organization</u> <ul style="list-style-type: none"> <li>- mobile industry (phone builders/ service providers)</li> <li>- the individual (memory and dissimulating)</li> <li>- Bank : online recording of operations</li> <li>- Transport company : machine (If PIN outside tel)</li> </ul>	Trust	The user considers himself/herself as a possible liability in the system security breakdown.
Offline User valid	<u>technology, individual, organization</u> <ul style="list-style-type: none"> <li>- mobile industry (phone builders/ service providers)</li> <li>- the individual (memory and dissimulating)</li> <li>- Bank : deferred recording of operations</li> <li>- Transport company : machine (If PIN outside tel)</li> </ul>		The a priori setting of the payment function makes the user responsible for the system security.
Offline PIN	<u>technology, individual, organization</u> <ul style="list-style-type: none"> <li>- mobile industry (phone builders/ service providers)</li> <li>- the individual (memory and dissimulating)</li> <li>- Bank : deferred recording of operations</li> <li>- Transport company : machine (If PIN outside tel)</li> </ul>		The user considers himself/herself as a possible liability in the system security breakdown. However, the offloading to the bank would be deferred, which reduced the feedback.
Offline without PIN	<u>technology, individual, organization</u> <ul style="list-style-type: none"> <li>- mobile industry (phone builders/ service providers)</li> <li>- the individual (memory et dissimulating)</li> <li>- Bank : deferred recording of operations</li> <li>- Transport company : machine (If PIN outside tel)</li> </ul>	Confidence	The user has no choices but relying on the device or not using it.

COPRIM	31.08.09	Consortium COPRIM	V 3.0	18/39
Project	Date	Author	Version	page

The more the user is involved, the more structuring is trust. This notably implies the user to be aware of threats to his/her privacy and at the same time it is enabling him/her to monitor an individual privacy management.

When the user has no choice but relying on the device confidence is here dominant. This causes the user's automatic exclusion from any monitoring of privacy. It also means that in case of failure, the user cannot be considered as a potential liability (see offline without PIN's option for example)<sup>7</sup>.

Considering these cases in the light of NFC expected commitments, we can assume that whereas the PIN code involves the user in the privacy management, its main drawback comes from the fact that it could seriously slow down the communication process. Yet, NFC's advantages are notably based on the communication speed and easiness of use. By contrast, the Offline user valid option seems to give the user a more efficient way of managing the privacy but requires him to be constantly aware of its security management.

## 4.2 Transport ticketing

### 4.2.1 Detailed description

Validating an electronic ticket only require the user to pass his NFC phone in front of the validating device. An audio and/or luminous signal informs customers that validation was successfully registered or that a problem occurred.

Three general solutions are considered:

#### 4.2.1.1 Case 1: Validation with ID

This proposal is voluntarily close to existing solutions. In this scheme there is not much security in contactless cards as they are linked to their owner by an identifying number. This allows the transport company to process an offline fraud checking (user ubiquity, over intensive usage, tickets double spending...)

In this case a card holds the following content:

- Card ID (linked to owner)
- Secret value (for authentication)
- Subscription slot
  - Name and biometric data
  - Rights on the transport network
  - Duration
- Ticket slots
  - Rights on the transport network
  - Ticket ID
- Last validation and timestamp with MAC

The protocol used for communication between the NFC and the reader is ISO/IEC 14443 Type B.

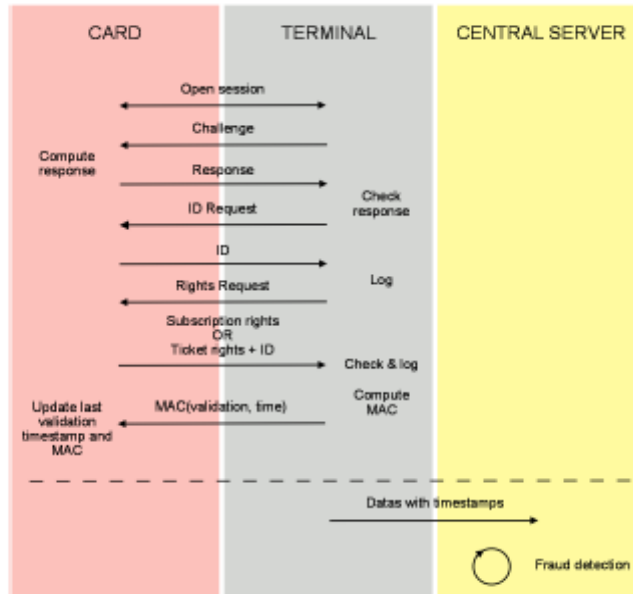
(In case where the transport application is embedded in a smart card connected to the NFC device, we consider the communication between the card and the NFC device is done through the S2C protocol).

<sup>7</sup> All use case analyses are based on the same grid.

COPRIM	31.08.09	Consortium COPRIM	V 3.0	19/39
Project	Date	Author	Version	page

## 4.2.1.1.1 Title Validation

Title validation proceeds in four times: card authentication, card identification, rights checking and MAC computation. A fifth step is processed offline: fraud detection.



The challenge/response phase provide dynamic card authentication. This prevents from card skimming. Challenge consists of a 128 bytes value and the response is this value encrypted with the secret value (AES128 CBC, IV=0). MAC is an AES128 CBC MAC.

## Threats:

- **Eavesdropping:** An attacker can here obtain data transmitted during validation as they are not encrypted. However, this does not enable him to create a copy of the card as he would need the secret value. Confidentiality is no more threatened as the attacker would need an access to the transport company database to link an ID to its owner.
- **Relay Attacks:** To mount such an attack, one could place a leech device close to the victim NFC phone and another could present the ghost to the reader at validation time. However, the gain for such an attack is very low compared to its complexity.
- **Denial of service and skimming:** As a contactless card responds every time she is brought in the field of a RF device, an attacker could use an antenna and a computer to simulate a validation device. In the case of tickets use, the card could so engage a validation process without the knowledge of its owner and spend his tickets.

COPRIM	31.08.09	Consortium COPRIM	V 3.0	20/39
Project	Date	Author	Version	page

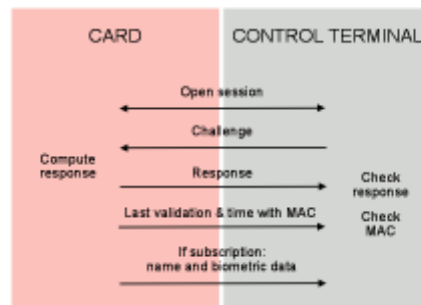
- **RFA:** In attacking the computation of the AES128 response, for instance by Radio Frequency Power Analysis, the attacker could retrieve the card secret value (see scenario 1). This could allow card skimming.
- **Tracing:** As card ID is known by the terminal and then backed up to a central server, users identification and tracing is possible. The transport company is able to know the exact travels of all its customers. This is a major issue about this proposal.

**Solutions:**

- **Relay attacks:** As previously, user validation (activation/deactivation) of NFC and/or distance bounding protocols could be applied.
- **Denial of service:** User NFC validation prevents from denial of service. The terminal could also have to authenticate itself to the card before the card accepts to complete the validation process.
- **RFA:** To resist against Side Channel Analysis Attack, it is necessary to protect algorithms implementations.
- **Tracing:** Organizational solutions have to be considered in order to prevent from customers tracing. A neutral and third party organization (ex : governmental) shall ensure that personal data are deleted after fraud detection and that they cannot be used for a tracing purpose.

**4.2.1.1.2 Title control**

Title control needs the user to present its NFC phone in front of the control staff portable device. Transaction is depicted below :



The card authenticates itself and then transmits the last validation recorded along with the MAC. In case of a subscription, owner name and biometric data are transmitted. The control staff can thus verify user identity and biometric data (photograph, fingerprint).

**Threats:**

Previous threats and solutions apply to control scheme excepting:

- **Denial of service:** does not apply.
- **Eavesdropping:** In case of a subscription, eavesdropping leads to a privacy threat as personal data (name, photograph or fingerprint) are transmitted.

COPRIM	31.08.09	Consortium COPRIM	V 3.0	21/39
Project	Date	Author	Version	page

- Skimming: An attacker could simulate a control device in order to obtain customer personal data against his will/knowledge.

Solutions:

- Eavesdropping: transaction encryption prevents from passive eavesdropping.
- Skimming: User NFC validation prevents from unwanted transaction. Control terminal authentication prevents from an attacker to simulate a control terminal

#### 4.2.1.2 Case 2: Validation without ID

This scheme relies on contactless cards security. If they are considered tamper proof, there is no need for the transport company to perform fraud detection, thus card IDs could be removed.

In this case a card holds the following content:

- Secret value (for authentication)
- Subscription slot
  - Name and biometric data
  - Rights on the transport network
  - Duration
  - Credential over name, biometric data, subscription rights and duration signed with transport company private key
- Ticket slots
  - Rights on the transport network
  - Counter
- Last validation and timestamp with MAC

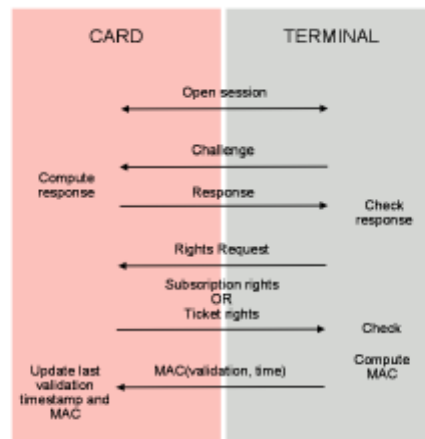
##### 4.2.1.2.1 Title validation

Title validation proceeds in three times: card authentication, rights checking and MAC computation.

The challenge/response phase provide dynamic card authentication. This prevents from card skimming. Challenge consists of a 128 bytes value and the response is this value encrypted with the secret value (AES128 CBC, IV=0). MAC is an AES128 CBC MAC.

COPRIM	31.08.09	Consortium COPRIM	V 3.0	22/39
Project	Date	Author	Version	page





## Threats:

- **Eavesdropping:** An attacker can here obtain data transmitted during validation as they are not encrypted. However, this does not enable him to create a copy of the card as he would need the secret value.
- **Relay attacks:** To mount such an attack, one could place a leech device close to the victim NFC phone and another could present the ghost to the reader at validation time. However, the gain for such an attack is very low compared to its complexity.
- **Denial of service:** As a contactless card responds every time she is brought in the field of a RF device, an attacker could use an antenna and a computer to simulate a validation device. In the case of tickets use, the card could so engage a validation process without the knowledge of its owner and spend his tickets.
- **RFA:** In attacking the computation of the AES128 response, for instance by Radio Frequency Power Analysis, the attacker could retrieve the card secret value (see scenario 1). This could allow card skimming.

## Solutions:

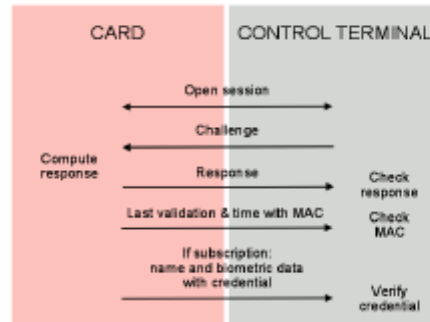
- **Relay attacks:** As previously, user validation (activation/deactivation) of NFC and/or distance bounding protocols could be applied.
- **Denial of service:** User NFC validation prevents from denial of service. The terminal could also have to authenticate itself to the card before the card accepts to complete the validation process.
- **RFA:** To resist against Side Channel Analysis Attack, it is necessary to protect algorithms implementations.

## 4.2.1.2.2 Title control

COPRIM	31.08.09	Consortium COPRIM	V 3.0	23/39
Project	Date	Author	Version	page

As previously, the user presents his NFC phone in front of the control staff portable device.

#### 4.2.1.2.2.1 Biometric data verified outside the smart card



The card authenticates itself and then transmits the last validation recorded along with the MAC. In case of a subscription, owner name and biometric data are transmitted along with the credential signed by transport company private key. Credential is checked, the control staff can then verify user identity and biometric data (photograph, fingerprint).

#### Threats:

Previous threats and solutions apply to control scheme excepting:

- Denial of service: does not apply.
- Eavesdropping: In case of a subscription, eavesdropping leads to a privacy threat as personal data (name, photograph or fingerprint) are transmitted.
- Skimming: An attacker could simulate a control device in order to obtain customer personal data against his will/knowledge.

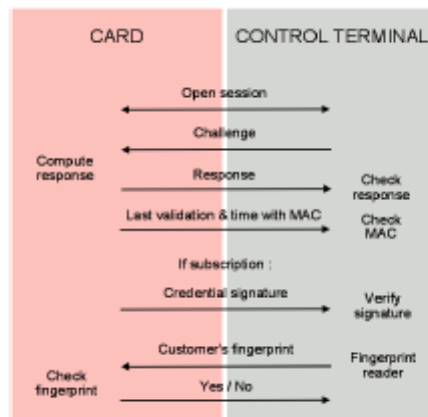
#### Solutions:

- Eavesdropping: transaction encryption prevents from passive eavesdropping.
- Skimming: User NFC validation prevents from unwanted transaction. Control terminal authentication prevents from an attacker to simulate a control terminal

#### 4.2.1.2.2.2 Biometric data verified inside the smart card

This particular scheme requires the use of a biometric data such as a fingerprint that a smart card can efficiently verify.

COPRIM	31.08.09	Consortium COPRIM	V 3.0	24/39
Project	Date	Author	Version	page



The card authenticates itself and then transmits the last validation recorded along with the MAC.

In case of a subscription, credential signature is verified by the control terminal. In this case, customer is then asked to use the terminal fingerprint reader which sends the fingerprint to the card. The latter check whether the fingerprint belong to the subscriber or not and returns "yes" or "no".

Fingerprint control could be replaced by identity control: the customer must present identity papers in order to prove his name to the control staff. Control staff then asks the card if the customer's name is the subscriber name. The card's answer is "yes" or "no".

#### Threats:

Previous threats and solutions apply to control scheme excepting:

- Denial of service: does not apply.
- Eavesdropping: In case of a subscription, eavesdropping leads to a privacy threat as personal data (name or fingerprint) are transmitted from the terminal to the card.
- Skimming: As the card never sends personal data, skimming does not apply.

#### Solutions:

- Eavesdropping: transaction encryption prevents from passive eavesdropping.

#### 4.2.1.2.3 Remarks

This proposal (i.e. "Case 2: Validation without ID") is designed as low cost solution: NFC applications are only required to perform private key (symmetric) cryptography. This can be achieved with relatively cheap smart cards. On the other hand, this solution needs private keys to be copied both on cards and on terminals which raise security issues. Moreover, the described scheme does not permit a user to prove (i.e. convince a third party actor) he bought a ticket or the company to prove a particular ticket was spent.

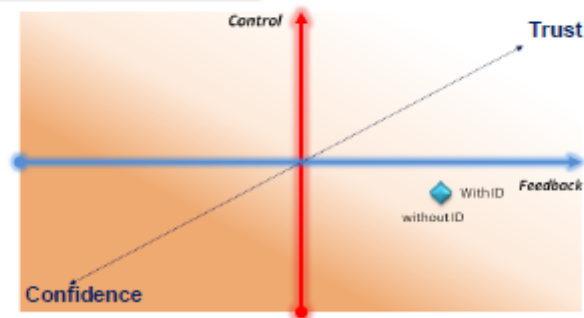
One can conceive another solution "Validation without ID" relying on public key cryptography with use of Zero-Knowledge Interactive Protocols (ZKIP). Such a solution would be much secure as the

COPRIM	31.08.09	Consortium COPRIM	V 3.0	25/39
Project	Date	Author	Version	page

compromise of a private key does not put in jeopardy the whole system. The drawback of this kind of solution is that it requires smart cards to perform public key cryptography in an efficient way as transport requirements are particularly harsh (a transaction should last at most 150m). This point makes this solution probably too expensive from the business model point of view.

#### 4.2.2 Analysis

##### Transport (validation) cases



	Delegation of responsibility for security	Prevailing type of Confidence	Protection failure offloading process
With ID	<p><u>technology, organization</u> Individual,</p> <ul style="list-style-type: none"> <li>- mobile industry (phone builders/ service providers)</li> <li>- the individual</li> <li>- Transport company :</li> </ul>	Trust	The user considers himself/herself as a possible liability in the system security breakdown.
Without ID	<p><u>technology, organization</u> Individual,</p> <ul style="list-style-type: none"> <li>- mobile industry (phone builders/ service providers)</li> <li>- the individual</li> <li>- Transport company</li> </ul>		The user considers himself/herself as a possible liability in the system security breakdown.

COPRIM	31.08.09	Consortium COPRIM	V 3.0	26/39
Project	Date	Author	Version	page

The two technical options show no substantial differences to the user because they are transparent to him/her. Both of them are offering the user a minimum amount of control and feedback that allows thinking that Trust would be at the center of the user/device relationship. However, post use concerns can arise specifically when considering the first option (with ID): tracing issues have already proved to be central for the acceptability of RFID related technologies.

#### 4.3 Smart poster (contactless token)

##### 4.3.1 Detailed description

The Smart Poster contains an URL in a tag. Once an NFC phone is passed in front of the poster with NFC activated, the NFC chip (in reader mode) reads this URL and sends it to the baseband processor. Then, Julie can obtain some information about the concert on the web for example or Yves can buy a ticket.

The protocol used for communication between the NFC and the reader is ISO/IEC 14443 Type B. It corresponds to the NFC Type 4 among the protocols defined by the NFC forum.

##### 4.3.1.1 Basic solution

The URL is simply read by the NFC phone and sent to the baseband processor.



Threats: An attacker can modify the tag or replace it by another one. Thus the following threats have to be considered:

- Phishing : the URL may be modified, and point at a malicious website
- Spamming, DOS (Denial of service): the URL may be modified, and point at a website of another announcer. This may also happen if someone takes a tag on a poster, and put it on another poster.

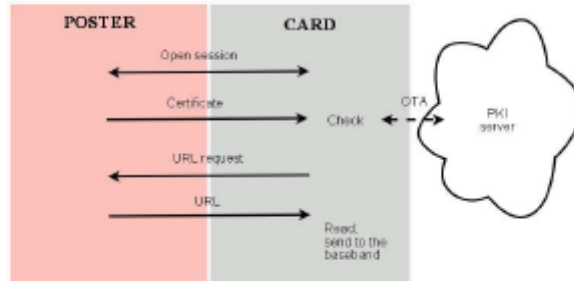
Solutions:

- The URL is displayed by the phone, and the user verifies it before validating the sent to the baseband.
- Other solutions are detailed in the next sections

COPRIM	31.08.09	Consortium COPRIM	V 3.0	27/39
Project	Date	Author	Version	page

#### 4.3.1.2 Solution with certification of the tag

Each tag (on a poster) is certified by a known authority. The NFC chip verifies the certificate, and authorize (or not) the next step. If necessary, part of that verification (check for revocation lists for example) could be achieved over the air (OTA) – i.e. using 3G communication.



##### Threats:

- Spamming, DOS (Denial of service): An attacker could take a (valid) tag on a poster, and put it on another poster.

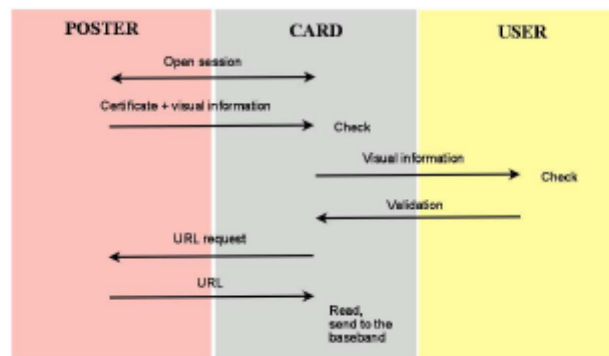
##### Solutions:

- The tag contains some visual information corresponding to (or to a specific part of) the poster, and sends it to the screen of the phone for a user validation. This solution is detailed in the next section.

#### 4.3.1.3 Solution with certification and consistency control by the user

After verification of the certificate by the NFC ship, the user verifies that the visual information sent to the screen of the phone corresponds to (or to a specific part of) the poster.

COPRIM	31.08.09	Consortium COPRIM	V 3.0	28/39
Project	Date	Author	Version	page



## Threats:

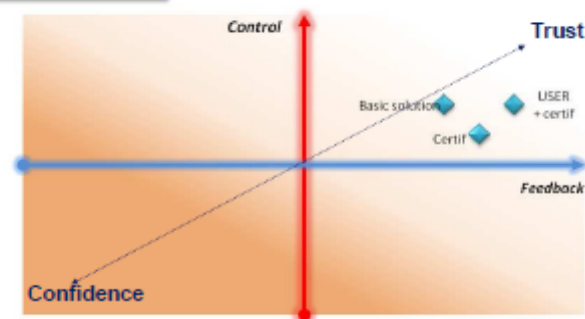
- Malicious software: A virus/trojan installed on the phone operating system (OS) could intercept the visual information and replace it by another.

## Solutions:

- Malicious software: Anti-virus software trusted computing (see TCG), hardware link between SE/NFC and screen.

## 4.3.2 Analysis

## Smart poster cases



COPRIM	31.08.09	Consortium COPRIM	V 3.0	29/39
Project	Date	Author	Version	page

	Delegation of responsibility for security	Prevailing type of Confidence	Protection failure offloading process
Basic solution	<u>technology, organization</u> <ul style="list-style-type: none"> <li>- mobile industry (phone builders/ service providers)</li> <li>- the individual (memory et dissimulating)</li> <li>- Transport company : machine and employees</li> </ul>	Trust	The user considers himself/herself as a possible liability in the system security breakdown.
Certif	<u>technology, organization</u> <ul style="list-style-type: none"> <li>- mobile industry (phone builders/ service providers)</li> <li>- the individual (memory et dissimulating)</li> <li>- Transport company : machine and employees</li> <li>- Certifying organization</li> </ul>		The user considers himself/herself as a possible liability in the system security breakdown.
User + Certif	<u>technology, organization</u> <ul style="list-style-type: none"> <li>- mobile industry (phone builders/ service providers)</li> <li>- the individual (memory et dissimulating)</li> <li>- Transport company : machine and employees</li> <li>- Certifying organization</li> </ul>		The user considers himself/herself as a possible liability in the system security breakdown. In that case, his/her involvement is more important than in the two previous others.

The three technical options are here very close and all of them involve a trust based relationship. However, we can notice some interesting differences between them. The basic solution and the User+certif. one offers a similar level of control that is higher than the certif. ones. This is explained by the fact that the user should necessarily rely on a certificate upon which he/she has no control. However, in the user+certif. case, the user regains a higher level of control thanks to its consistency control. Once again, a tradeoff is to be made here between the user involvement and the NFC's commitments. Finally, as all options are considered to rely on a trust relationship, it is important to note that they all put the user at the centre of this case. The question is therefore: what kind of skills are we expecting the user to develop to manage a risk proof and privacy-enhanced communication?

COPRIM	31.08.09	Consortium COPRIM	V 3.0	30/39
Project	Date	Author	Version	page



#### 4.4 Device pairing (peer to peer)

##### 4.4.1 Detailed description

We propose a solution to enhance the security of device pairing using Bluetooth technology. First of all we briefly describe the case without use of a NFC chip, and then we present our solution.

Bluetooth wireless technology is a short-range communication system intended to replace the cables connecting portable and/or fixed electronic devices.

Pairing is an important part of Bluetooth. It's how two devices - a phone and a headset, for example, or two phones - associate themselves with one another. A shared secret is generated, and used for all future communication. Pairing is why, when on a crowded subway, your Bluetooth devices don't link up with all the other Bluetooth devices carried by everyone else. According to the Bluetooth specification, PINs can be 8-128 bits long. Unfortunately, most manufacturers have standardized on a four decimal-digit PIN (in order to be easily entered by a user in two devices, or exchanged between two users).

##### Threats:

- Eavesdropping: As the used PIN code is not very long (for practical reasons), it is possible to perform eavesdropping on the communication and then recover the PIN by brute force or dictionary attack. This enables then to decrypt the whole communication.

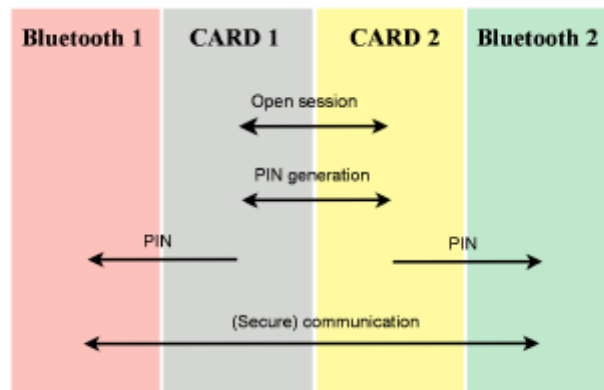
##### Solutions:

- Eavesdropping: The first part of the pairing is executed using NFC chips. Thus a (long) PIN is quickly generated (without any intervention of users) and the communication is more secure.

The proposed solution is then the following: once two Bluetooth NFC Phones are placed close together (a few centimeters) with NFC activated, those devices enter in pairing mode (with a possible user validation). PIN is then generated by the two NFC devices and exchanged. Bluetooth communication is then initiated using this value.

One can note that this process simplifies Bluetooth usage : users don't care anymore about PIN and avoid menus navigation in order to activate Bluetooth.

COPRIM	31.08.09	Consortium COPRIM	V 3.0	31/39
Project	Date	Author	Version	page



## Threats:

- Relay attacks (see previous cases)
- Eavesdropping: If PIN is exchanged in plaintext mode, eavesdropping can be performed and can lead to the whole communication decryption.

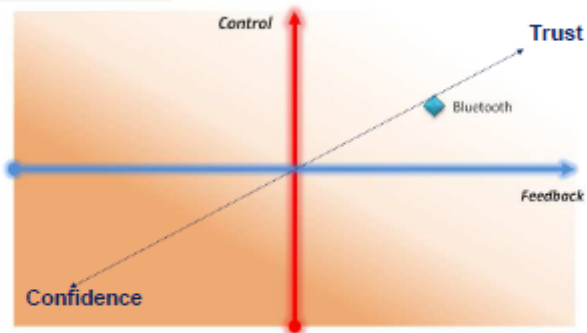
## Solutions:

- Relay attacks: As previously, user validation (activation/deactivation) of NFC and/or distance bounding protocols could be applied.
- Eavesdropping: A secure Diffie-Hellman key exchange prevent from eavesdropping.

COPRIM	31.08.09	Consortium COPRIM	V 3.0	32/39
Project	Date	Author	Version	page

4.4.2 Analysis

## Device pairing cases



	Delegation of responsibility for security	Prevailing type of Confidence	Protection failure offloading process
Bluetooth	technology, organization - mobile industry (phone builders/ service providers) - the individual (memory et dissimulating) - the other Bluetooth user	Trust	The user considers himself/herself as a possible liability in the system security breakdown.

Bluetooth is assumed here to be the unique solution. Trust is here involved only if we consider the validation function to be... functional.

COPRIM	31.08.09	Consortium COPRIM	V 3.0	33/39
Project	Date	Author	Version	page

## 5 Conclusion

### 5.1 On the scenarios design and description

For each of the four scenarios we tried to propose different implementations. These propositions do not aim at being exhaustive but cover a wide range of possibilities in terms of security, privacy and control given to the user.

It is worth noting that each scenario implementation allows furthermore a set of independent countermeasures that could be controlled or not by the end user. It could be for example: configuration of the NFC device allowing or not NFC transaction based on several criterions (PIN authentication, activity detection, timeout...). We did not mention those possible additional protections in the implementations since they lie on an orthogonal axis (in the sense that this axis is independent from scenarios implementation choices).

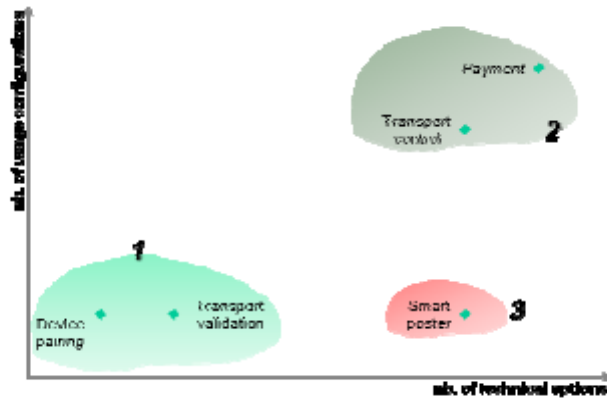
Finally we have to mention the particular status of the last scenario. As its description is strongly linked to the technological layer, it does not allow any room for prospecting. We are thus reduced to analyze the only possible implementation of device pairing. On the other hand, independent countermeasures presented above apply to this scenario as the others.

### 5.2 Analysis summarizing part

It seems important to notice that beyond the technical options inherent to each use case, those analyses fail in providing us with a comparative and relational overview of all of the use cases. Indeed, as the COPRIM project aims to "validate on relevant scenarios [its] primitives of protection of the private life [of the user]", pursuing this goal required the building of a tool – as incomplete as it could be – that gives us a plain view of the use cases. Therefore, we chose one of the project's main targets as the issue that could help us to transcend the very contingency of each case. We try to assess the use cases according to the amplitude of the technical available options' impact on privacy management. In other words, our goal is to evaluate whether design options gives room for manoeuvre (number of technical options per use case, *x* axis) and if this room for manoeuvre challenges the prospective use in various ways (number of use configurations involved, *y* axis). The unhelpful side of such a tool is here obvious in that it erases at the same time the control/feedback grid and the trust/confidence factors. This advocates for understanding this analysis as necessary complementary of the previous one<sup>8</sup>. Furthermore, the following analysis should not be understood as a prediction of the use potential and economical fate of each use cases. It has been built upon the project's previous production and numerous interactions between the project's partners.

<sup>8</sup> This also indirectly questions the latent link established during the project between the control/feedback level and the expected acceptability of the CPM...

COPRIM	31.08.09	Consortium COPRIM	V 3.0	34/39
Project	Date	Author	Version	page



Thus, the chart shows 3 categories of use cases. (1) Device pairing and transport validation cases both offer few technical options – one for the former, two for the latter, and those are moreover restricted to only one use configuration. The opposite category (2) groups together the payment and transport control cases. They both offer multiple technical options distributed amongst different use configurations: in particular, the payment case knowing larger amplitude whatever the variable is. Finally the smart poster case (3) does have as many options as the transport control's one but those all belongs to only one use configuration.

Linking this grid with the role of design in the project, we could conclude that the choices made in (2) and (3) are to be carefully thought upon because these cases contain a large amplitude of the available technical options' impact on privacy management. At the opposite, the (almost) unidirectional path that design can take for (1) allows to think that these use cases are less challenging when the social is considered to be at stake to evaluate the technical choices' pertinence. Furthermore, as regards the users' opinions toward the CPM, working on (1) exclusively would involve that acceptability testing would focus upon one inflexible proposition whereas different options for the same use case could be proposed and tested towards users during this latter stage of the project.

Finally, as agreed during the beginning of the project, we reproduced the sequential cutting of the scenario. However, it is remained undecided if the scenario should include all phases or a restricted selection of them.

COPRIM	31.08.09	Consortium COPRIM	V 3.0	35/39
Project	Date	Author	Version	page

## 6 Appendix

### 6.1 Sociologic tools

#### 6.1.1 Bellotti Gird

	Feedback about	Control Over
Capture	When and what information about me gets into the system	When and what not to give out what information; I can enforce my own preferences for system behaviours with respect to each type of information I convey
Construction	What happens to information about me once it gets inside the system	What happens to information about me. I can set automatic default behaviours and permissions
Accessibility	Which people and what software have access to information about me and what information they see or use	Who and what has access to what information about me. I can set automatic default behaviours and permissions.
Purposes	What people want information about me for. Since this is outside the system, it may only be possible to infer purpose from construction and access behaviours.	It is infeasible for me to have technical control over purposes. With appropriate feedback, however, I can exercise social control to restrict intrusion, unethical, and illegal usage.

From (Bellotti, 2001).

### 6.2 Cryptographic protocols and algorithms

#### 6.2.1 SDA (Static Data Authentication)

The Card transmits its IPK (Issuer Public Key) certificate and a signature of static data to the terminal for validation.

SDA provides data integrity because the issuer has digitally signed Important data on the ICC, which the terminal authenticates.

Weakness:

The signed static data can be skimmed from a valid card and put in another one.

#### 6.2.2 DDA (Dynamic Data Authentication)

DDA provides additional benefits compared to SDA since it allows the terminal to verify the authenticity of the Card. In a DDA transaction, the Card creates a unique digital signature for each transaction, using the Rivest, Shamir, Adleman (RSA) algorithm or the Elliptic Curve Digital Signature Algorithm (ECDSA). Then terminal checks that this dynamic signature is valid and, therefore, that the card is genuine. Because the Card needs to be able to perform RSA cryptography to generate this dynamic signature, DDA cards normally cost more than SDA cards.

Successful DDA provides assurance that the card is genuine and not counterfeit.

#### 6.2.3 RSA (Rivest Shamir Adleman)

The RSA cryptosystem is the widely used Public Key cryptosystem.

Assume that Bob wants to send a message to Alice.

COPRIM	31.08.09	Consortium COPRIM	V 3.0	36/39
Project	Date	Author	Version	page

**Key Pair Generation:**

Alice selects two large prime numbers  $p$  and  $q$  and computes their product :  $N = p \cdot q$ .

Then, she chooses  $e$  with  $0 < e \leq N$  and  $\text{pgcd}(e, \varphi(N)) = 1$  where  $\varphi(N) = (p-1)(q-1)$ .

She computes  $d$  with  $0 < d \leq N$  and  $ed = 1 \bmod \varphi(N)$ .

At last, we have:

Public Key:  $(N, e)$   
Private Key:  $(p, q, d)$

**Encryption:**

Bob has to parse his message in blocks of  $n = \log_2 N$ -bits.

Each message block  $M$  of  $n$  bits is encrypted by computing  $C = M^e \bmod N$ .

**Decryption**

Alice received  $C$ . She computes  $C^d = M \bmod N$ .

Indeed, we have:

$$\begin{aligned} C^d &= (M^e)^d \bmod N \\ &= M^{e \cdot d} \bmod N \\ &= M \bmod N \end{aligned}$$

**RSA Signature**

Suppose Alice uses Bob's public key to send him an encrypted message. Bob has no way of verifying that the message was actually from Alice since anyone can use Bob's public key to send him encrypted messages. So, in order to verify the origin of a message, RSA can also be used to sign a message.

Suppose Alice wishes to send a signed message to Bob. She can use her own private key to do so.

She uses Bob's private key to cipher her message and computes her signature in this way:

She produces a hash value of her message:  $\text{hash}(M)$  and computes  $S = (\text{hash}(M))^d \bmod N$  (as she does when decrypting a message).

When Bob receives the signed message, he decrypts the message with his private key and uses the same hash algorithm.

He computes  $S^e \bmod N$  (as he does when encrypting a message to Alice) and compares the resulting hash value with the message's actual value.

If the two agree, he knows that the author of the message was in possession of Alice's secret key, and that the message has not been tampered.

**6.2.4 ECDSA (Elliptic Curve Digital Signature Algorithm)**

ECDSA is a variant of the Digital Signature Algorithm (DSA) which operates on elliptic curve groups.

**Signature Generation Algorithm**

Suppose Alice wants to send a signed message to Bob. Initially, the curve parameters  $(q, F, a, b, G, n, h)$  must be agreed upon. Also, Alice must have a key pair suitable for elliptic curve cryptography, consisting of a private key  $d_A$  (a randomly selected integer in the interval  $[1, n-1]$ ) and a public key  $Q_A$  (where  $Q_A = d_A G$ ).

Alice wants to sign a message  $M$ , she follows these steps:

COPRIM	31.08.09	Consortium COPRIM	V 3.0	37/39
Project	Date	Author	Version	page

1. Calculate  $e = \text{hash}(M)$ , where hash is a cryptographic hash function, such as SHA-1.
2. Select a random integer  $k$  from  $[1, n - 1]$ .
3. Calculate  $r = x_1(\text{mod } n)$ , where  $(x_1, y_1) = kG$ . If  $r = 0$ , go back to step 2.
4. Calculate  $s = k^{-1}(e + rd_k)(\text{mod } n)$ . If  $s = 0$ , go back to step 2.
5. The signature is the pair  $(r, s)$ .

**Signature verification algorithm**

Bob wants to authenticate Alice's signature, he must know her public key  $Q_k$ . He follows these steps:

1. Verify that  $r$  and  $s$  are integers in  $[1, n - 1]$ . If not, the signature is invalid.
2. Calculate  $e = \text{hash}(M)$ , where hash is the same function used in the signature generation.
3. Calculate  $w = s^{-1}(\text{mod } n)$ .
4. Calculate  $u_1 = e.w(\text{mod } n)$  and  $u_2 = rw(\text{mod } n)$ .
5. Calculate  $(x_1, y_1) = u_1G + u_2Q_k$ .
6. The signature is valid if  $r = x_1(\text{mod } n)$ , Invalid otherwise.

**6.2.5 DES (Data Encryption Standard)**

DES for Data Encryption Standard is a NIST standard (NBS, 1977). It is the most used cryptographic algorithm in the world.

It is a Block Cipher designed by IBM which has been selected as standard for encryption by the NIST in 1976: cf. DES\_FIPS\_PUB\_46-3. Its structure is a Feistel scheme with 16 rounds which takes as input a 64-bit plaintext and returns a 64-bits cipher text. It uses a 64-bit secret key.

**6.2.6 AES (Advanced Encryption Standard)**

AES (NBS, 2001) has been chosen as the new encryption standard by the NIST in October 2001 after a study made on many candidates provided by many institutes worldwide. It is not a Feistel scheme contrarily to the DES, however it is a SPN for Substitution Permutation Network, so it is based on rounds based on substitution and permutation operations. It resists to actual theoretical cryptanalytic attacks.

There are 3 possible key sizes for AES in the NIST standard. Plain and cipher texts are 128 bits long but the key size can be 128, 192 or 256 bits. Depending on the key size the number of rounds  $Nr$  for the AES varies:

- message of 128 bits and key of 128 bits:  $Nr = 10 \Rightarrow$  cipher text of 128 bits,
- message of 128 bits and key of 192 bits:  $Nr = 12 \Rightarrow$  cipher text of 128 bits,
- message of 128 bits and key of 256 bits:  $Nr = 14 \Rightarrow$  cipher text of 128 bits,

All the operations are done in the field of characteristic 2:  $\text{GF}(2^8)$ .

COPRIM	31.08.09	Consortium COPRIM	V 3.0	38/39
Project	Date	Author	Version	page



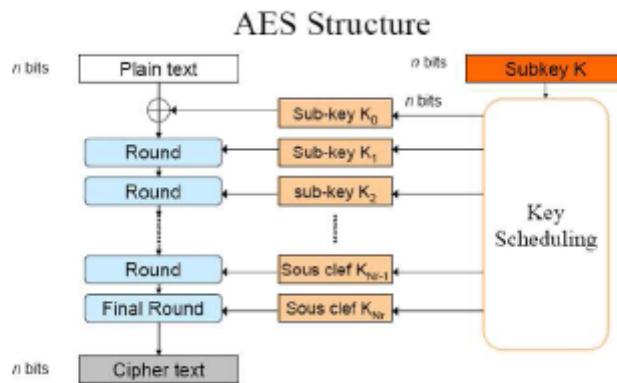


Figure 1 AES encryption.

## 7 Bibliography

- Belotti, V. (2001). Design for Privacy In Multimedia Computing and Communications Environments. [auteur du livre] P.E. et Rotenberg. *Technology and Privacy: The New Landscape*. Cambridge : The MIT Press, 2001, pp. 63-98.
- NBS, National Bureau of Standards. (2001). *FIPS 197, Advanced Encryption System (AES)*. 2001.
- . (1977). *FIPS PUB 46, Data Encryption Standard (DES)*. 1977.
- Dourish P., Grinter R., Delgado et Joseph M. (2004). « Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem », *Personal and Ubiquitous Computing*, vol. 8, no° 6, p. 391-401.
- Luhmann N. (2001). « Confiance et familiarité. Problèmes et alternatives », *Réseaux*, vol. 4, no° 108, p. 15-35.
- Marx G.T. (2001). « Murky Conceptual Waters: the Public and the Private », *Ethics and Information Technology*, vol. 3, no° 3, p. 157-169.
- Samarajiva R. (2001). « Interactivity As Though Privacy Mattered », In Agre, P.E. et Rotenberg, M. (éd.) (2001). *Technology and Privacy: The New Landscape*, The MIT Press, p. 277-310.

COPRIM	31.08.09	Consortium COPRIM	V 3.0	39/39
Project	Date	Author	Version	page

## **Annexe 4.**

### **Technical Annex**

**COPRIM**  
**(COn tactless PR ivity Manager)**

**Technical Annex**

**Type de projet:** Recherche industrielle

**Axes thématiques:**

**Principal :** Sécurité pour les télécommunications et les réseaux  
**Secondaire :** Réseaux Auto-Organisants et Objets Communicants

**Durée:** 36 mois

**Partenaires:**

CEA-LETI  
INSIDE CONTACTLESS  
UVSQ/PRISM  
UPMF

## Table of contents

<b>1. PROJECT</b>	<b>3</b>
1.1. RESUME EN FRANÇAIS	3
1.2. ABSTRACT IN ENGLISH	5
1.3. INTRODUCTION	7
1.3.1. Overview of the project	7
1.3.2. Scientific challenge	7
1.3.3. Technical challenge	7
1.3.4. Economic challenge	8
1.3.5. Societal challenge	8
1.3.6. Bottlenecks	8
1.3.7. Expected outcome	8
1.3.8. Application perspectives	9
1.3.9. Relevance with the call	9
1.4. CONTEXT AND STATE OF THE ART	10
1.4.1. Project position & national international competition	10
1.4.2. Economical context	15
1.4.3. Market analysis	15
1.4.4. Contactless and Privacy standardization works	16
1.5. PARTNERSHIP	17
1.5.1. Partners presentation	17
1.5.2. Involvement in other related projects: complementarities and synergies	19
1.6. PROJECT ORGANIZATION AND RESOURCES	21
1.6.1. Work package breakdown	21
1.6.2. Work packages and tasks description	23
1.6.3. Added value of collaboration	37
1.6.4. Management structure	37
1.6.5. Risks assessment	38
1.6.6. Main milestones and deliverables	38
1.6.7. Main project reviews	38
1.6.8. Planning of work packages and tasks	40
1.6.9. Manpower resources per task and per partners	41
1.7. EXPECTED RESULTS AND PERSPECTIVES	43
1.7.1. Project objectives & expected outcome with evaluation criteria for success measurement	43
1.7.2. Scientific and applications perspectives	44
1.7.3. Relation with existing standards	45
1.8. INTELLECTUAL PROPERTY	45
<b>2. FINANCIAL RESOURCES</b>	<b>47</b>
2.1.1. Manpower and budget	47
2.1.2. Justification of personnel, equipments, traveling, operating costs	47
2.1.3. Other public funding of the project	48

## 1. Project

### 1.1. Résumé en français

Le déploiement rapide des systèmes sans contact fait que ces derniers font d'ores et déjà partie des produits électroniques utilisés quotidiennement par des millions de personnes. On peut prendre comme exemple le domaine des transports publics. Ces dispositifs représentent une catégorie de composants numériques qui sont à la base de la future Intelligence Ambiante : cartes à puce et étiquettes RFID. Par ailleurs, à partir de standards existants du domaine de la carte puce (ISO 14 443 et ISO 15 693), un standard générique regroupant ces standards et les produits sans contact les plus répandus de la bande ISM 13.56 MHz a émergé : le standard NFC (ECMA 340 & 352, ISO 18092). NFC est le sigle retenu pour « Near Field Communication », c'est-à-dire pour les produits fonctionnant en couplage inductif, et donc à courte portée contrairement au sans fil. Notons qu'aujourd'hui ce standard est en cours de déploiement sur l'ensemble des téléphones portables. Ce qui augmente d'autant plus la diffusion et l'utilisation de cette technologie sans contact.

Cependant une certaine inquiétude s'est faite jour auprès des utilisateurs de la technologie sans contact concernant la protection de la vie privée. En effet ces systèmes sans contact peuvent être potentiellement l'objet d'actions malveillantes cherchant à mettre en défaut de façon consciente ou inconsciente la confidentialité des données échangées. En outre la caractéristique des objets sans contact est que ces actions peuvent avoir lieu sans que le propriétaire de l'objet en soit informé, donc à son insu. Sans mesures de protection particulières le concept d'Intelligence Ambiante peut tracer quelqu'un.

Contrairement au problème de sécurité du lien sans contact qui sont liés à la lutte contre la fraude économique intentionnelle, les problèmes de protection de la vie privée concernent la manipulation des données personnelles ou dévoilant une information non souhaitée par son propriétaire. Pour accéder à un service on doit dévoiler son identité à l'opérateur qui lui souhaite protéger ses accès. Etre piqué en permanence voire pillé plus ou involontairement par les dispositifs électroniques liés à l'Intelligence Ambiante soulève un autre problème : celui de pouvoir proposer à l'utilisateur la création d'une sphère privée autour de lui afin de s'isoler du monde numérique et de garder son anonymat. Il faudra cependant veiller à ce que cette déconnexion ne soit pas sujette à provoquer des situations de déni de service.

Le but du projet COPRIM est de proposer des solutions pertinentes et viables sur le plan économique, afin de redonner le plein contrôle à l'utilisateur et par cela à maintenir la confiance qu'il porte à ces objets électroniques.

Le projet a 4 axes de travail majeurs :

- proposer des primitives de solutions technico-économiques de protection de la vie privée des systèmes de type NFC
- (re)donner confiance à l'utilisateur dans les produits sans contact (NFC)
- établir un business model de diffusion des primitives de protection de la vie privée
- valider sur des scénarios pertinents ces primitives de protection de la vie privée.

Les défis techniques :

- Surveillance permanente de l'environnement électromagnétique à 13.56MHz (NFC)
- Détection de tentative de connexion à l'insu du porteur

- Gestion de barrières physiques et protocolaires pour le contrôle des accès par l'utilisateur
- Contraintes dues aux objets portables à faibles ressources énergétiques et de traitement

Les résultats attendus :

- Meilleure vision des besoins des systèmes NFC en terme de protection de la vie privée
- Compatibilité des mesures de protection de la vie privée avec les fonctions de sécurité
- Réduction des possibilités de détournement des fonctions de protection de la vie privée pour provoquer du déni de service
- Business model en relation avec celui du NFC
- Maintien de la confiance des utilisateurs dans les objets portables sans contact de type NFC

## 1.2. Abstract in English

The fast deployment of contactless systems makes that they are already part of the electronic products used daily by millions of people. One can take as example the public transport domain. These devices represent a category of digital components which are at the base of the future Ambient Intelligence: smart cards and RFID tags. Starting from existing smart cards standards (ISO 14 443 and ISO 15 693), a generic standard grouping these standards and the most widespread contactless products of ISM band 13.56 MHz has emerged: the NFC standard (ECMA 340 & 352, ISO 18092). NFC stands for "Near Field Communication", i.e. for the products functioning in inductive coupling, and thus with short range contrary to wireless devices. Let us note that today this standard is in the course of deployment on the mobile phones. What all the more increases the diffusion and the use of this contactless technology.

However a certain concern arose from the users of the contactless technology concerning the protection of the private life. Indeed these contactless systems can be potentially the object of malicious actions trying to jeopardize the confidentiality of the exchanged data. Moreover the characteristic of the contactless objects is that these actions can take place without the owner of the object being informed, therefore without its awareness. Without protection measures the concept of Ambient Intelligence can trace somebody.

Contrary to the security problem of the contactless link which is related to the fight against the intentional economical fraud, the problem of protection of the private life relates to the handling of the personal data or revealing information not desired by its owner. To get a service one must reveal his identity to the operator who wishes him to protect his accesses. To be tracked permanently even to be plundered more or less involuntarily by the electronic devices related to the Ambient Intelligence raises another problem: be able to propose to the user a deprived sphere around him in order to isolate himself from the digital world and to keep its anonymity. It will have however to be taken care that this disconnection is not prone to cause situations of deny of service.

The main goal of the COPRIM project is to propose relevant and viable solutions from the economical point of view, in order to give again the full control to the user and by that to maintain the confidence which he carries to these electronic objects.

The project has 4 major axes of work:

- to propose technico-economical primitives of solutions of protection of the private life of the systems of t NFC type
- To give confidence to the user in the contactless products (NFC)
- to establish a business model for diffusion of the primitives of protection of the private life
- to validate on relevant scenarios these primitives of protection of the private life.

Technical challenges:

- Permanent monitoring of the electromagnetic environment at 13.56MHz (NFC)
- Detection of attempt of connection without the knowledge of the holder
- Management of physical and protocol barriers for the control of the access by the user
- Constraints due to the portable objects with low energy and processing resources

Expected results:

- Better vision of the needs for NFC systems in term of protection of the private life
- Compatibility of the protection measures of the private life with the security
- Reduction of the possibilities of malicious use of the functions of protection of the private life for deny of service
- Business model in relation to that of the NFC
- Maintenance of the confidence of the users in the contactless portable objects of the type NFC



### 1.3. Introduction

#### 1.3.1. Overview of the project

The main goal of the project is to secure from relevant threats the transfer of private data information to and from contactless portable devices that communicate within the near field component of the electromagnetic field. Because of national power emission regulations and economical and technical trade-off, these devices work basically in the HF frequency band (i.e. 13.56 MHz ISM band). Today, these devices include mainly contactless smart cards and RFID electronic tags. Except data communication ciphering and authentication at protocol layers for smart cards, they do not support protection functions to prevent hostile remote passive eavesdropping, remote device activation and relay attacks. Because these so called contactless nomadic devices will be extensively used in the next future, economical but efficient protection functions have to be introduced in short term.

The objectives of the project are double:

- a) to protect privacy data of persons or companies from contactless privacy threats
- b) to maintain trust and confidence of the citizens through the extensive use of a private Contactless Privacy Manager (CPM).

The work will stress mainly on the protection of identity and personal data in the context of P2P, P2M and M2M communications.

#### 1.3.2. Scientific challenge

Near field communication systems use the near field electromagnetic field part of the electromagnetic field to communicate. Because the magnetic field component of this near field is larger than the electric one, proximity power transfer is possible using magnetic coupling. Power transfer is performed with a high frequency band carrier (typically 13.56 MHz) through the couple of antennas which is a very low efficient transformer and data communications are implemented through the modulation of the carrier.

Remote and relevant threats may arise also from distances which are no more in the classical range of near field model, but not yet relevant of the far field. This "intermediate field" requires much more attention than today current attention and has to be a little bit more modeled and checked versus remote hostile scenarios. In particular, long range emission of the reader antennas must be modeled, because today antenna are designed and optimized for near field usage, without worrying long range radiation components of the electromagnetic field except for respecting local regulations. Reversely, excitation modes of device antennas are not extensively studied when designed and no quantized information at design level is available to know how far it is possible to activate a near field device.

#### 1.3.3. Technical challenge

The technical objective is to define and design a low cost device that controls and processes any contactless transaction in the surroundings of the user. Data communications are implemented through two basic layers: physical link and protocol layer. The technical challenge will be to use both layers to detect and prevent from hostile threats. Cross layer approach seems to be very relevant. Any information coming either from the radio frequency link or from the exchanged messages have to be fused to have an as complete as possible real time situation awareness system.

In a hostile context, the portable device will have to trigger protections and counter measures that will be compatible with the limited available resources. Low power and low cost solutions must be targeted.

Moreover, to increase trust and confidence of the user, it seems very relevant that this device must be a stand alone one, fully controlled by the user. It must be its own and personal security resource for contactless devices management, in particular because of potentially unauthorized and covert remote hostile activation.

#### 1.3.4. Economic challenge

The economical challenge is double:

- Firstly the protection extra cost must be compatible with mass production products and consumers society markets.
- Secondly, added protection functions must booster the sales volumes of portable contactless devices according to the degree of confidence of the customers, users and citizens.

#### 1.3.5. Societal challenge

Two main societal challenges are foreseen, one at the person level and the other at the digital society level:

- Protect the privacy of the citizen/customer
- Enable the largest used of near field portable devices

Another key point is the way of introduction of the secure feeling among users. Two technical and practical approaches are basically in competition for a business model:

- protection functions add ons on existing devices with privacy functions offered by usual devices manufacturers and usual operators (Embedded CPM: E-CPM)
- unique and personal extra device coming from independent manufacturing and distribution circuits (Stand alone CPM: SA-CPM)

The way to introduce privacy function is a key challenge of the COPRIM project.

#### 1.3.6. Bottlenecks

Technical bottlenecks are:

- Facing a large set of potential threats in continuous evolution
- Limitations of processing capabilities of passive and very low cost portable devices
- Realistic economical extra cost for the CPM device (SA-CPM)
- Potential modification of existing equipments: readers and portable devices (E-CPM)
- Lack of international standards on Privacy Enhancement Technologies devoted to contactless

#### 1.3.7. Expected outcome

a) Core technical outcome

A set of hardware and software protections or mixed functions including:

- Real time contactless threats situation awareness
- Controllable countermeasures fully triggered by users with full observability and audit

- Contribution to Contactless Privacy Enhancement Technologies standards

b) Extra technical knowledge:

- Connection with national privacy organizations (CNIL in France) (law and regulation compatibility)
- Connection with existing standards (standard and regulation compatibility)

Business model (economic compatibility)

### 1.3.8. Application perspectives

a) For the smart cards segment (P2P or P2M)

- E-banking
- E-citizen
- E-health
- E-government
- Entertainment

b) For the automatic identification capture (P2M or M2M)

- RFID
- Traceability
- Localization

### 1.3.9. Relevance with the call

The objectives of this project are relevant mainly with Thème 5: "Sécurité pour les télécommunications et les réseaux"

Basically, the project is a "Recherche industrielle" project and will focus on the following sub items:

- "Systèmes d'identité numérique"
- "Outils de confiance pour protéger la chaîne des services associés"
- "Systèmes et mécanismes de protection de la sphère privée"
- "Systèmes et dispositifs de traçabilité"

#### 1.4. Context and State of the Art

##### 1.4.1. Project position & national international competition

###### Project context 1) Digital world and privacy

With the trumpeted arrival of Ambient Intelligence (AmI), digital data privacy is a key point. Several low resources smart devices have shown some connections with privacy concerns:

- RFID electronic tags for items identification
- e-Citizen contactless cards (e-passport, e-identity, ...) for person identification

In that "privacy situation", the main drawback of these contactless systems is that there is no switch on/switch off mechanism to assess the will of the owner to use them. They can be remotely and covertly activated and triggered without the awareness of the owner.

Privacy is the ability of an individual or group to keep their lives and personal affairs out of public view, or to control the flow of information about them. It is clear that AmI may endanger the privacy of citizens. On the other hand, AmI aims to offer a lot of on-line services that you can get only if you identify yourself or the items you are dealing with. So the difficulty.

Basically, the CPM security module should be a stand alone and personal device. Another usage is to incorporate some of its security functions both on the reader and on the portable device. However for RFID electronic tags, the goal is not to have an over cost of these very low cost devices, and the stand alone solution looks better, from an economical point of view.

The ideal stand alone CPM must integrate the following minimum functions:

- A- Contactless environment sensing
  - a. Detection of all known contactless standard activities (smart cards and RFID tags)
  - b. Real time situation awareness of surrounding readers (friend or foe)
- B- Black lists management
  - a. Implicitly authorized readers
  - b. Implicitly authorized contactless devices
  - c. Controlled devices (readers or cards or tags) unknown or not
- C- Basic communication controller
  - a. Control of every data exchange between personal devices and readers
  - b. Interception of the full messages
- D- Communication jammers for private sphere
  - a. Blocking unwanted communication through jamming
  - b. Counter measures against eavesdropping
- E- Identity manager
  - a. ID controller
  - b. Anonymity management
  - c. Personal data management
- F- Authentication manager
  - a. Authentication function between readers and low resources devices (RFID tags) where authentication is not supported

- b. Authentication of readers
- G- Friendly user interface
  - a. On line display of every messages
  - b. On line control of every data exchange
- H- Audit memory
  - a. Recording of every transaction
  - b. Off line Display of every transaction
- I- Auto destroy
  - a. CPM auto destruction
  - b. Contactless device destruction
  - c. Management of kill function

A range of CPM devices may be envisioned, starting from the simplest Faraday case for one card to a full featuring device.

It is not in the intent of the project to cover this full range of privacy functionalities. However, conceptual studies and CPM specifications will take into account the full range of possibilities. The project will select a subset to be implemented into the demonstrators. Four functions are basically planned, but the final focus of the project could be slightly re-oriented after the full analysis phase. So far, the last three do not seem to be relevant today to R&D project but are relevant of integration of existing technologies.

The prioritized items targeted by the COPRIM project and addressed by the partners are:

- A: Contactless environment sensing (LETI, INSIDE, UPMF)
- D: Communication jammers (LETI, INSIDE, UPMF)
- E: Identity manager (UVSQ, INSIDE, UPMF)
- F: Authentication manager (UVSQ, INSIDE, UPMF)

#### *RFID electronic tags*

The concept of ambient intelligence (or *AmI*) is a vision where humans are surrounded by computing and networking technology unobtrusively embedded in their surroundings. The privacy concerns have been raised very early with the introduction of RFID smart devices. In particular the introduction and potential generalization of electronic tags on mass markets products and so on for every shop or supermarket have enlarged the potentiality of person traceability. The interoperability of automatic data capture systems and the combination of tagged items on a person may be used to trace this person when moving in commercial center or urban areas.

#### *e-Citizen contactless cards*

Concerns are also very high with the use of contactless e-passport. Some hostile distant reader may check your nationality and trigger attacks.

A same scheme may be ruled out with a contactless identity card.

High sensitive privacy personal data may be potentially downloaded from contactless health cards without the agreement of the owner.

### **Project context 2) Contactless and Privacy research works**

Many proposals have been presented, essentially from research laboratories. Among them we may point out:

#### *Faraday cage*

The purpose of the Faraday cage is to stop electromagnetic field. It is used as a very low cost shield mechanism. It is a very simple approach, and thus proposes only a very partial solution for privacy concerns. This basic solution confines the RFID tags in a wallet made of a metallic sheet or mesh. This wallet plays the part of a Faraday cage blocking the HF and UHF radio signals of readers. The efficiency is certain but this approach is inefficient for a large and spread set of tags.

#### *Blocker tags*

The "blocker tags" exploits a characteristic of RFID communication: the search tree protocol a reader uses to determine which tags it sees. The blocker tag works by always responding to the reader query and emulating all the possible ID set. In this way, it can serve to passively jam the reader, forcing the reader to endlessly inventorying very large virtual trees.

Furthermore, this approach may be assimilated to deny of service. However a normal reader can detect malicious use of blocker tags by checking the too large number of presumed present tags (over 1000 for example) or by checking the inconsistency of some ID numbers with what subset it is expected to be read.

#### *RFID Guardian*

The RFID Guardian is a system that allows people to administer the security of their RFID tags. It is an academic project developed at Vrije and Delft universities in the Nederland. The RFID Guardian is a mobile battery-powered device that offers personal RFID security and privacy management for people. The RFID Guardian monitors and regulates RFID usage, on the behalf of consumers. The design of the RFID Guardian was driven by the following goals:

- Centralized use and management: Most existing RFID countermeasures distribute their security policies across RFID tags, which make them very hard to configure, manage, and use. To address this concern, the Guardian is a single platform to leverage RFID countermeasures in a coordinated fashion. Personalized security policies are centrally enforced by utilizing novel RFID security features (auditing, automatic key management, tag-reader mediation, off-tag authentication) together with existing ones (kill commands, sleep/wake modes, on-tag cryptography).
- Context awareness: Different countermeasures have strengths and weaknesses in different application scenarios. Low cost RFID tags require different access control mechanisms than expensive crypto-enabled contactless smart cards. The Guardian maintains both RFID-related context as well as personal context
- Ease-of-use: People do not want to fuss with an RFID privacy device, so the Guardian aims to be both physically and operationally unobtrusive.

Unfortunately, some proposed solutions are not consistent with the complete security and confidentiality. One counter measure proposed by the Guardian is to emit a signal to disturb the CRC (Cyclic Redundancy Check) of a message frame when emitted by the tag at the end of the ID code in order to invalidate reading of the incoming ID message by the reader. It is nice for normal readers but nevertheless an eavesdropper can still listen to the ID code. The protection is highly not sufficient from a confidentiality and privacy point of view.

#### *EM Field Context awareness*

The first point is that the user be continuously aware of the electromagnetic context to early detect any reader activity. The second point is that this detection can be very accurate, contrarily to basic readers,



because the receiver bloc of the sensing system has no carrier to emit but only to listen the traffic at 13.56 MHz. So the signal to noise ratio measurement to detect abnormal physical characteristics is much better than the one of a basic reader. Many other electromagnetic parameters can be managed and processed: SNR, timing, EM signature, magnetic coupling, etc.

#### *The Watchdog tag*

Floerkemeier and al. [7] describe a device named "watchdog" tag that has the functionalities of a tag but may be incorporated in a mobile phone or a PDA. The "watchdog" tag is an audit system for RFID privacy that monitors the readers in the vicinity. Thus, if a reader scans your personal tags, the "watchdog" tag displays on the screen the intrusion attempt and the features of the reader. This kind of device is only able to make you aware of the danger but it is ineffective of removing it.

#### *Antenna energy analysis approach*

This solution is based on the assertion that distance implies distrust. The closer the reader is, the more subject it is to be uncovered by the holders, owners and/or users of the tagged object. To enhance privacy, RFID tags might be able to employ the signal-to-noise ratio of the transmissions they receive from a reader to estimate the distance of that reader from the tag. Then tag answers or not the requests of the reader depending on this distance. This kind of approach is efficient but destroys an important interest of RFID which is the long distance reading.

#### *Tag destruction or similar countermeasures*

A Kill command has been introduced in ePC electronic tags (equivalent for RFID tag to the EAS labels destruction) to inhibit definitively the tag to prevent any ID code emission. This solution consists of creating a new command, the "kill" command that enables the destruction of the tag that can never be re-activated. The deactivation can be made with a fuse on the power supply of the chip or on the antenna, or with the erasing of the memory. This command should be used at the checkout of the store. This approach, defended by the consumers' associations, solves all the problems of privacy. But, outside the supply chain all the advantages of RFID disappear. Thus, the future view of the Ambient Intelligence becomes quite reduced: no more possibility to make fridges discuss with food or washing-machine with clothes. Even the control of a part of the supply chain is removed. The tracking of items for recycling or for after-sale services is no more feasible. With such an approach, RFID only remains a tool to improve logistics of manufacturers and distributors.

#### *The clipped tag*

Responding to RFID privacy concerns, IBM has developed a "clipped tag" technology, offering consumers the ability to tear or scratch off RFID antennae, eliminating the threat of an un-authorized reading of the tag. ePC has created a standard that includes a "kill" command to make RFID tags inoperable altogether. But that action, once taken, cannot be reversed. This would present a problem when consumers return items to the store — the RFID tag could not be read at all. With the clipped tag technology, though the antenna would be inoperable, the tag could still be read if held directly to an RFID reader, according IBM. This process puts the choice of privacy in the hands of consumers. It provides visual evidence that the tags have been modified, important psychologically to those concerned about RFID privacy, but does not totally destroy the tag.

#### *The encryption approach*

This approach uses cryptographic methods incorporated in the tag to protect privacy while ensuring the desired functionalities. This approach does not follow the trend of the cutting down of the cost of tag. Today, a 5 cents cost is targeted for a tag (antenna plus chip) that does not seem compatible with the increasing number of transistors required for cryptographic algorithms. Three different techniques appear in the literature:

- The "Hash-Lock" approach: In this solution, a tag can be "locked" with no more possibility to answer its ID until it will be unlocked. The tag is locked by a code  $y$ , and it is only unlocked by presentation of a key or PIN value  $x$  such that  $y=h(x)$  for a standard one-way hash function  $h$ . This approach requires as well a randomization in the hash function not to track items with their value  $y$ . The main drawback for the consumer is the waste of time unlocking his shopping basket.
- The re-encryption approach: This solution appeared when Juels and Pappu [8] try to solve the privacy implications of tracking RFID tags of banknotes. Their banknotes are encrypted with a law-enforcement public key. A periodic re-encryption of the ciphertexts is required to lower the risk of linkability of different appearances of a given tag. This encryption is provided by public privacy-enhancing readers in stores since each RFID tag has reduced computing resources. The cost for installing such a network of readers is the main problem to face.
- Silent tree-walking: This approach is an answer to the threat of passive eavesdroppers hearing the signal broadcasted by the reader that may be possible picked up very far from, contrary to the signal transmitted by the tag that is really weaker. In deterministic singulation protocol, for example the tree-walking algorithm often used in the RFID standards to avoid that different tags answer together, the reader calls tags by a part of their UID and increase the number of bits until it finds a single tag. Thus, by listening to the reader, we may know a part of the UID of each tag. To prevent those attacks, the tags are able to generate their own random pseudo-IDs before singulation. Nevertheless, the authors did not measure the impact of the increase in the number of transistors on the cost of the tag when manufacturers make drastic effort to reach a price of 5 cents for a tag.

#### Consumers associations

Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN) is a consumer group fighting retail surveillance schemes since 1999. With thousands of members in all 50 U.S. states and over 30 countries worldwide, CASPIAN seeks to educate consumers about marketing strategies that invade their privacy and to encourage privacy-conscious shopping habits across the retail spectrum.

Faced with the reaction of the consumers, RFID might be nipped in the bud. To find solutions to ensure privacy of people with RFID, it's important to define in straightforward terms the different fears around RFID tags. Three main reasons of RFID rejection cannot be ignored:

1. Tag reading without the user consent and awareness, or eavesdropping of the communication
2. Every device is traced (unique code for each product that is, taken alone, insignificant)
3. Each unique code (and so, each item) is a pointer to a database which can be linked to the owner (by credit card number for example) or to other unique codes (so other items) that enable to identify the owner or profile him.

Solutions that try to defend privacy around RFID systems should do away with these three facts or should supervise them.

#### CNIL

CNIL is a French public organization devoted to privacy for citizen against the emerging of new information and communication technologies. Of RFID is a main concern. The technology of radio-



identification (RFID) becomes a major economic stake in particular in the applications of the distribution and transport. Because of their massive dissemination, individual nature of the identifiers of each marked object, of their invisible nature, and risks of shaping of the individuals, the CNIL considers that RFIDs are personal identifiers within the meaning of the law "Informatique and Libertés".

#### References :

- [1] Privacy Protection for Secure Mobile RFID Service  
Doo Ho Choi et al. IEEE 2006
- [2] Ari Juels, Ronald L. Rivest, Michael Szydlo, The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy, CCS.03, October 2003.
- [3] Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest, and Daniel W. Engels, Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems, First International Conference on Security in Pervasive Computing (SPC) 2003.
- [4] Some Methods for Privacy in RFID Communication  
K. Fishin et al. IBM ESAS 2004
- [5] A Platform for RFID Security and Privacy Administration  
Melanie R. Riaback et al., Vrije Universiteit, 2006
- [6] S. E. Sarma, S. A. Weis, and D.W. Engels, Radio-frequency identification systems. In Burton S. Kaliski Jr., C. et al. Kaya Koç, and Christof Paar, editors, *CHES '02*, pages 454–469. Springer-Verlag, 2002. LNCS no. 2523.
- [7] C. Floerkemeier, R. Schneider, and M. Langheinrich. (2004) Scanning with a purpose—Supporting the fair information principles in RFID protocols. [Online]. Available: [citeseer.ist.psu.edu/floerkemeier04scanning.html](http://citeseer.ist.psu.edu/floerkemeier04scanning.html)
- [8] A. Juels and R. Pappu. Squealing Euros: Privacy protection in RFID-enabled banknotes. In R. Wright, editor, *Financial Cryptography '03*. Springer-Verlag, 2003.

#### 1.4.2. Economical context

It is difficult to quantify the economic impact of the fraud. But this is an important concern for the governments. Various projects are targeting the security issues and many organizations already decided to move from "papers" to "electronic documents". This important modification is also providing the market users with additional applications capabilities and for the security aspect at least a step to authentication capability.

Fraud in the banking application is well known, and important organizations such as Gie-Bancaire, VISA or Master Card are strongly involved in the risk management at the global level. In the ID market, the passport became the first example of widely deployed document and the first feedback addressing security issues are published in various circumstances. The main target of this project is to find a solution to improve the protection of the smart card and associated products access based on signature management and authentication. The security level is one of the main issues in the deployment of such new applications and could be a solution to leverage the spreading of this new technology

#### 1.4.3. Market analysis

The smartcards and portable electronic devices are more and more used in various domains. After the communication, the new market drivers are the banking applications and the e-

government, such as the passports and ID cards. Those new domains are much more sensitive, because many data related to "privacy" and/or money access data are embedded in such documents.

The NFC technology is also providing the market with new approaches capability. Then the market is quickly moving from "paper" management (Money ID cards, Driving license, etc.) to "virtual document".

#### 1.4.4. Contactless and Privacy standardization works

##### *Contactless standards*

COPRIM partners are currently involved in contactless standards such as ISO SC17 (Contactless Smart Cards) and ISO SC31 (Electronic Tags).

##### *Privacy related standards*

New initiatives have been started by the European Commission, which has established a formal Expert Group on RFID. This group is currently working to issue an European Recommendation on "Privacy and Security" by the end of 2007. CEN TC 225, and so ISO CN31, are involved in the works. Proposal of evolution of existing standards by introducing PET aspects is currently under way.

## 1.5. Partnership

### 1.5.1. Partners presentation

#### Inside Contactless

Established in 1995, INSIDE Contactless is a fabless semiconductor provider, specifically dedicated to contactless memory chips, microprocessors and readers. Based in France with representations in the US, Singapore, China and Poland, company provides its products towards cards manufacturers and embedders.

INSIDE Contactless core business is to conceive and sell its products, thus having control on all IP areas. As a result, emphasis has always been strong on R&D, way before contactless markets began to really take off, thus ensuring in present days a high level of expertise and knowledge of all contactless-related constraints, concepts and norms.

Key facts for INSIDE Contactless include:

- 100+ staff
- 55 patents since inception
- 250 customer portfolio worldwide
- Products are used in various fields such as mass-transit, ID, payment, access control.
- 96% of turnover made overseas
- Growth rate 50% per year.
- Inside microprocessors have been displayed at more than 13M units worldwide
- 50%+ market share in Contactless payment in the USA.

The next level for INSIDE Contactless is to use its expertise and skills towards the development of NFC technologies. The cumulated experience gained over the years allows the company to position itself as an active contributor in this field. Several pilot projects involving NFC technologies are currently displayed involving INSIDE Contactless alongside partners such as SFR, Credit Mutuel, NRJ Mobile, Sagem Monetel, Gemalto, Sagem Communication, MasterCard, and AIRTAG. INSIDE Contactless is also a member of the NFC Forum which aims at defining standards of this nascent industry.

#### UVSQ/Prism

The cryptology team of the PRISM laboratory was born in 2001, with Jacques Patarin, grew in 2004 when Louis Goubin and Antoine Joux joined it. Michaël Quisquater recently joined the trio.

In its research activities, the cryptology team aims at widely covering the various themes of academic research in cryptology, public key and secret key cryptography, cryptanalysis, security of implementations, number theory, multivariate cryptography, hash functions, etc.

The cryptology team brings its specificity in the computer science courses at UVSQ and, since several years, the university offers several teaching programs with a part devoted to cryptology and information security. In particular, the research graduate program "Applied

Algebra" offers a full cryptology course. It has just been complemented by a professional graduate program, called SeCReTS (Security of Contents, Networks, Telecommunications and Systems).

In order to contribute to the national and international renown of the team, its members give a significant time to research management. In particular, there are currently ten PhD students within the team: four are working in the PRISM laboratory at UVSQ, and six are working in computer science companies.

Moreover, the members of the team published many papers about physical attacks. Among the most important are:

- [1] P. Delaunay, A. Jour : « Galois LFSR, Embedded Devices and Side Channel Weaknesses ». In Proceedings of INDOCRYPT 2006, LNCS, Springer-Verlag, 2006.
- [2] M.-L. Akkar, R. Bevan et L. Goubin : « Two Power Analysis Attacks against One-Mask Methods ». In Proceedings of FSE'2004, LNCS, Springer-Verlag, 2004.
- [3] M.-L. Akkar, L. Goubin et O. Ly : « About an Automatic Fault Injection Protection System ». In Proceedings of E-Smart'2003, Nice, 2003.
- [4] M.-L. Akkar et L. Goubin : « A Generic Protection against High-Order Differential Power Analysis ». In Proceedings of FSE'2003, LNCS, Springer-Verlag, 2003.
- [5] L. Goubin : « A Refined Power-Analysis Attack on Elliptic Curve Cryptosystems ». In Proceedings of PKC'2003, LNCS 2567, pp. 199-211, Springer-Verlag, 2003.
- [6] L. Goubin : « A Sound Method for Switching between Boolean and Arithmetic Masking ». In Proceedings of CHES'2001, LNCS 2162, pp. 3-15, Springer-Verlag, 2001.
- [7] J.-S. Coron et L. Goubin : « On Boolean and Arithmetic Masking against Differential Power Analysis ». In Proceedings of CHES'2000, LNCS 1965, pp. 231-237, Springer-Verlag, 2000.
- [8] L. Goubin et J. Patarin : « DES and Differential Power Analysis ». In Proceedings of CHES'99, LNCS 1717, pp. 158-172, Springer-Verlag, 1999.

#### CEA-LETI

The LETI is an applied research laboratory in electronics recognized world-wide by many industrialists who exploits a technology resulting from work of R&D of his teams. In the areas of contactless systems and secure components one can point out:

- 15 years of work of R&D in contactless systems (more than twenty patents). Development of industrial prototypes in the field of teleticketing (subway ticket, reader for terminals of entry), of contactless payment (readers and cards), of medical implants and RFID labels. Technology transfer towards industry.
- 7 years of security evaluation within the framework of the common criteria through the activity of a CESTI laboratory.
- Participation in standardization committees of ISO SC17 and SC 31 (contactless smart cards and electronic labels) since 1995 (AFNOR). Invited as a technical expert to take part in international meetings (ISO in particular)

The R&D activities of the LETI in the field of the protection of contactless devices are positioned on two main axes:

- The implementation of electronic secure functions into the reader-tags system
- The use of a specific and portable electronic device for secure control through its know-how and skills on RF air interface and secure components.

## CEA-LETI references:

- [1] « PEA Card or Power Embedded Active Card », E. Crochon et Al., e-Smart, Sophia-Antipolis France, 2004
- [2] « New Technologies for Contactless Air Interfaces », F. Vacherand et Al., e-Smart Sophia Antipolis France, 2005
- [3] « New Technologies for RFID », F. Vacherand., sOc-EUSAI'05 Grenoble France 2005

## UPMF

The Pierre Mendès-France University is specialized in social sciences. It is involved in development and research projects, such as ANR and EU-IST, with its UMAN Lab laboratory, created in January 2007. This team of multidisciplinary Technological Research is directed by professor Valerie Chanaal and gathers teams of research which focus their works on the processes of innovation in the technological development

Two teams of UMAN Lab will contribute to the COPRIM project:

- Sociology of the user, team directed by the sociologist Philippe Mallein. Since 1996 this team has been developing and applying the CAUTIC method (Design assisted by the use for technologies, innovation and change) which is used to design new applications and innovative services by considering the user at the most early stage in the process of development. This method was used in the study and the technological development of solutions by several industrial companies and within the framework of national and European R&D projects.
- New markets and business model, team directed by the professor in management Valerie Chanaal. This team is currently developing new methods for management of the technological innovations, to anticipate the structure of the new markets and to plan the strategy within the framework of the new markets

## UPMF references:

- [1] F. Forest, L. Arhippainen: "Social Acceptance of Proactive Mobile Services- Observing and Anticipating Cultural Aspects by a Sociology of User Experience Method", SOC-EUSAI, 12-14 october, 2005, Grenoble, France
- [2] L. Arhippainen, F. Forest: "Future Proactive Services for Everyday Life", DNSCIT, 2006, Medina, Spain.
- [3] F. Forest, A. Oehme, K. Yaici, C. Verchere-Morice: "Psycho-Social Aspects of Context Awareness in Ambient Intelligent Mobile Systems", Workshop, 15th IST Summit 2006, Mykonos, Greece
- [4] K. Yaici, F. Forest, A. Oehme: "e-SENSE - Translating User Requirements into Technical Requirements for Ambient Intelligent Mobile Systems", Workshop, 16th IST Summit 2007, Budapest, Hungary

### 1.5.2. Involvement in other related projects: complementarities and synergies

## CEA-LETI:

CEA-LETI is involved in FP6 IST-Discreet project.  
The project aims to define technical solutions to support the introduction of new mobile/ubiquitous services by addressing the related privacy issues. The goal is to minimize and control the amount of personalized information made available to the involved organizations, in order for the users to benefit of services without worrying about dissemination and improper use of their personal data. This project is mainly software/middleware oriented. The role of LETI is to make RFID tags compatible with the approach.

CEA/LETI is also involved in the ODYSSEE project: The main goal of this project is to analysis, to select and to secure a hardware implementation of stream cipher algorithms. These cryptographic blocs will be part of the future communicating objects of Ambient Intelligence.

#### UVSQ:

UVSQ is involved in the following projects:

CrySCoE (ANR / ARA SSIA), from January 1st, 2006 to December 31st, 2008, is a consortium made up of ENS, Université Bordeaux I and UVSQ. This project has the ambition to extend the notions of security and attacks to the case of software programs executed in embedded systems (obfuscation, authenticity of code, etc.). The focus is placed on architectures where the executable code is provided by external means.

Odyssee (ANR / TLCOM), from March 1st, 2007 to February 28th, 2010, is a consortium made up of Gemalto, CEA-LETI and UVSQ. The main goal of this project is to select, analyze and secure the implementation of stream ciphers against physical attacks.

#### UPMF

In the field of the studies centered on the user (scenarios, user requirements, acceptability) the UPMF is involved in the French-Finnish ADAMOS research project, the European IST e-SENSE project, and project ANR-RNRT/LAM.

In the field of the business development and strategy, the UPMF drove the business aspects of the scenarios of the project IST e-SENSE and is also committed in several projects combining the problems of technological innovation and of economic and strategic intelligence. More largely, the UPMF is specialized in the expertise and the management of the processes of breakthrough innovation.

## 1.6. Project organization and resources

### 1.6.1. Work package breakdown

The COPRIM project is split into 5 work packages. The last one is devoted to project management.

The four first technical work packages are scheduled in three steps:

- Phase I: Privacy for contactless devices analysis (WP1)
- Phase II: Design of concepts and validation platform development
- Phase III: Privacy enhancement validation

Each work package and each task has a leader, between parentheses herein after. A work package leader is a member of the Steering Committee.

WP1: Privacy for contactless and threats analysis (UVSQ)

Task 1.1: Personal data and privacy use cases (UPMF)

Task 1.2: Contactless portable devices and threats analysis (LETI)

Task 1.3: Final specifications of targeted CPM protection functions (INSIDE)

WP2: CPM Design (LETI)

Task 2.1: Design of protection at physical level (LETI)

Task 2.2: Design of protection at protocol level (UVSQ)

Task 2.3: Cross layer design (INSIDE)

WP3: CPM Development (INSIDE)

Task 3.1: Demonstrator specifications (INSIDE)

Task 3.2: Demonstrator development (LETI)

Task 3.3: Demonstrator functional test and validation (INSIDE)

WP4: Security and privacy validation (INSIDE)

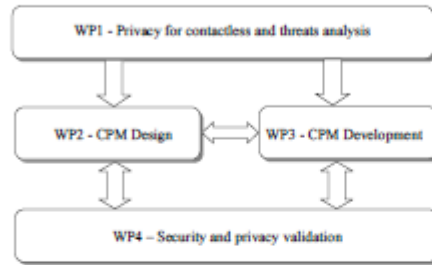
Task 4.1: Use case security demonstration (LETI)

Task 4.2: Use case privacy validation (INSIDE)

WP5: Project management (LETI)

Task 5.1: Project coordination (LETI)

Task 5.2: Results dissemination (UVSQ)



**Technical work package organization**



## 1.6.2. Work packages and tasks description

### WP1 : Privacy for contactless and threats analysis

a) Objectives: The goal of this work package is to analyze the main threats that jeopardize the privacy of the user of contactless devices.

b) Description :

The first goal of this work package is to inventory the different threats that are specific to the contactless devices. The second is to identify the requirements that should be mandatory for a protection device such as a CPM Contactless Privacy Manager. Finally the third step is to specify the CPM. This specification will have two aspects:

- a) the overall and global functionalities for an "ideal" protection device
  - b) what subset of functionalities will be practically developed in the project.
- The work will be organized around selected scenarios and use cases for their relevance with the goals of the COPRIM project.

The WP1 works will be split into 3 tasks:

- Task 1.1: Personal data and privacy use cases
- Task 1.2: Contactless portable devices and threats analysis
- Task 1.3: Final specifications of targeted CPM protection functions

c) Planning : T0 to T0+12

d) Deliverable : a report including the following items:

- State of the art on contactless threats versus privacy
- State of the art of current protection with drawback analysis
- Use cases and scenarios specification to tackle within the project

e) Expected results: This work package will deliver input for the WP2, WP3 and WP4 work package

WP1 Task 1	Title : Personal data and privacy use cases				
Start	T0	Duration	12 Months	Resources (m.m)	15
Partners	INSIDE	CEA-LETI	UVSQ	UPMF	
Effort in m.m	2	2	6	5	
Objectives : Analysis of personal data and privacy issues					
Description of work:					
Inventory of contactless threats and current protections					
Physical layer :					

<ul style="list-style-type: none"> <li>• Contactless link weaknesses</li> <li>• Use cases identification. Relationship with NFC Forum</li> <li>• Existing protections</li> </ul> <p>Protocol layer:</p> <ul style="list-style-type: none"> <li>• Protocol weaknesses</li> <li>• Authentication Issues</li> <li>• Existing protections</li> <li>• Attacks against the confidentiality of sensitive information</li> <li>• Problems related to the authentication of portable device and/or readers</li> <li>• Existing protections</li> </ul> <p>Use case definition</p> <ul style="list-style-type: none"> <li>• User requirements for privacy (trust and confidence)</li> </ul> <p>Demonstration scenarios</p> <ul style="list-style-type: none"> <li>• Scenarios relevance</li> <li>• Validation process for privacy assessment</li> </ul>			
Deliverable	Title	Date	Type
D 1.1.1	Scenarios and uses cases report	T0 + 12	Report
Validation criteria: Partners know how			

WP1 Task 2	Title : Contactless portable device and threats analysis				
Start	T0	Duration	12 Months	Resources (m.m)	14
Partners	INSIDE	CEA-LETI	UVSQ	UPMF	
Effort in m.m	3	4	6	1	
Objectives : Definition of the contactless portable device for threats protection					
Description of work:					
<p>The main goal of this task is to specify the protection functions and operating modes that will be mandatory for a contactless portable device. This analysis will be done within different constraints in mind:</p> <ul style="list-style-type: none"><li>• Stand alone autonomous portable device</li><li>• Contactless threats ranking</li><li>• User driven privacy control</li><li>• Operation modes</li><li>• Manufacturing and sales circuits</li><li>• Standardization Issues</li></ul> <p>- Remote passive eavesdropping scenario : the goal is to specify passive eavesdropping scenarios. Each scenario will comprise two elements: a target application and an attack. A synthetic document will give a global structure for the considered scenarios, sorted by criteria to be defined : type of attack, complexity of implementing the attack, cost, etc.</p> <p>- Active attacks with Intruder readers, or relay attacks : the goal here is to describe active</p>					

attacks using intruder readers, or relay mechanisms. We will study the state of the art of such attacks, with a particular focus on systems in which the contactless communicating object is used to prove the identity of a human being (identity documents, passports, ...). Two threats have to be specifically taken into account: identity borrow (e.g. with relay attacks), and identity theft (passive eavesdropping combined with intruder readers). In this context, we will also consider attacks that threaten privacy of citizens.

The main purpose is to offer an user friendly device to get and to keep the trust and confidence of the users. Very simple usage will be required with good performances and services.

The results of this investigation will be used to specify the CPM device.

Deliverable	Title	Date	Type
D 1.2.1	Analysis report	T0 + 12	Report

Validation criteria: Partners know how

WP1 Task 3 Title : Final CPM specification					
Start	T0	Duration	12 Months	Resources (m.m)	7
Partners		INSIDE	CEA-LETI	UVSQ	UPMF
Effort in m.m		3	4	0	0
Objectives : Specification of the Contactless Privacy Manager					
Description of work:					
<ul style="list-style-type: none"> <li>The main purpose of this task is to specify the CPM device. Embedded functionalities will be investigated in order to optimize their implementation. The global hardware architecture will be addressed in order to have a full overview of the device complexity. The investigation will take into account: relevance of the selected protection to be embedded</li> <li>Relationship between the high level specification and the technical options.</li> <li>economical feasibility</li> <li>standardization compatibility and perspectives</li> <li>autonomy issues</li> <li>degree of confidence feedback returned to the user</li> <li>potential misuse of some protection functions</li> <li>Industrial issues: manufacturing process, cost, etc...</li> <li>Manufacturing issues: techno, location, confidentiality</li> </ul>					
<p>Finally, this task will detail the sub set of protection functions that will be investigated and validated within the framework of the COPRIM project. It is intended to focus on the following functions:</p> <ul style="list-style-type: none"> <li>Contactless environment sensing</li> <li>Communication jammers</li> <li>Identity manager</li> <li>Authentication manager</li> </ul>					

Deliverable	Title	Date	Type
D 1.3.1	CPM Specification report	T0 + 12	Report
Validation criteria: Partners know how			

**WP2 : CPM Design**

a) Objectives: The goal of this work package is to design the different functions that will be included in the CPM device

b) Description : The main goal of this work package is to design the CPM device according to the specifications of task 1.3.

Each selected protection function will be designed and tested through experiments and dedicated test bench in order to validate the protection efficiency within specific scenarios. Optimization of hardware complexity and power consumption will be undertaken. Coherency and inter functions compatibility will be addressed. A continuous checking will be done to verify that these new privacy protection functionalities do not lower or the existing security functions.

The WP2 work are split into 3 tasks:

- Task 2.1: Design of protection at physical level
- Task 2.2: Design of protection at protocol level
- Task 2.3: Cross layer design

c) Planning : T0 to T0+24

d) Deliverable :

- CPM design report

e) Expected results: This work package will deliver input for the WP4 CPM development

WP2 Task 1	Title : Design of protection at physical level				
Start	T0	Duration	24 Months	Resources (m.m)	22
Partners	INSIDE	CEA-LETI	UVSQ	UMPF	
Effort in m.m	12	10	0	0	
Objectives : Design and development of the protections at physical layer					
Description of work:					
Development of sensing scanner and jamming counter measures at physical layer (PHY).					
Physical layer:					
<ul style="list-style-type: none"><li>• Sensing scanner</li><li>• Jamming countermeasures</li></ul>					
The sensing function will be devoted to the scanning of the HF spectrum for the detection of close readers in the surroundings of the CPM. This is a passive mode which listen all the current available standards that a user could potentially bear on him: ISO 14 443, ISO 15 693 and ISO 18000-3 which are the near field standards for smart cards or electronic tags.					
The jamming countermeasures are devoted to protect the privacy of the user either to avoid hostile eavesdropping or to increase the confidentiality of a communication.					
Deliverable	Title			Date	Type

D 2.1.1	Sensing and jamming functions report	T0+24	Report
Validation criteria: Partners know how			

WP2 Task 2	Title : Design of protection at protocol level				
Start	T0	Duration	24 Months	Resources (m.m)	9
Partners		INSIDE	CEA-LETI	UVSQ	UPMF
Effort in m.m		1	2	6	0
Objectives : Design and development of the protections at protocol layer					
Description of work:					
Development of secure protections at protocol level:					
a) Identity management					
b) authentication management					
c) personal data protection					
<p>In the context of passive attacks, a detailed study of the attacks described in Task T1.2 will be conducted, and adapted protections at the protocol level (software) will be proposed. A particular attention will be given to the two following points:</p> <ul style="list-style-type: none"><li>• Sensitive (static) data, specific to the contactless card owner (Identity, biometric data, ...)</li><li>• (Static or dynamic) data used for card authentication to the reader.</li></ul> <p>An analysis of the impact in terms of performances and memory constraints, if such protections are to be used, will be also provided.</p>					
<p>In the context of active attacks, a detailed analysis of the attacks described in Task T1.2 (active attacks scenarios) will be provided, and adapted protections at the protocol level (software) will be proposed. The two following problems will be particularly addressed:</p> <ul style="list-style-type: none"><li>• Preventing "man in the middle" attacks (relay attacks)</li></ul> <p>Mechanisms to prevent the use of a contactless card without its owner being aware of it</p> <p>An analysis of the impact in terms of performances and memory constraints of the proposed protections will be also provided.</p>					
Deliverable	Title			Date	Type
D 2.2.1	Protection at protocol level report			T0+24	Report
Validation criteria: Partners know how					

WP2 Task 3	Title : Cross layer design		
Start	T0+6	Duration 18 Months	Resources (m.m) 5
Partners	INSIDE	CEA-LETI	UVSQ UPMF
Effort in m.m	1	4	0 0
Objectives : To fuse information available at physical level and protocol level to improve threats			

detection and protection countermeasures			
Description of work:			
<p>This task will address two goals:</p> <ol style="list-style-type: none"> <li>1) enhancement of threats detection</li> <li>2) Improvement of countermeasures</li> </ol> <p>Based on the solutions from the WP2/Task2, the issues will be addressed in 2 ways: one by the protocol level and the second one by the embedded softwares in the devices and/or in the reader. The main processes which have to be fixed are mainly related to the eavesdropping and the relay attacks, but all the "regular" attacks for the contact technology are also providing efficient solutions to imagine hacking channels against such products.</p> <p>This task will also need improvement of existing side channel attacks countermeasures to be able to deal with the "authentication" needs to address those new applications.</p>			
Deliverable	Title	Date	Type
D 2.3.1	Report on cross-layer optimization	T0+24	Report
Validation criteria: Partners know how			

**WP3 : CPM Development**

a) Objectives: The goal of this work package is to integrate the CPM functionalities from the results of WP2 into a project demonstrator.

b) Description:

A first task of this work package is to specify the CPM demonstrator and use case scenarios for the final demonstration.

The second task is to integrate the privacy protection functions developed in WP2 into the CPM demonstrator.

The third task is to address functional tests of the CPM demonstrator.

When qualified, the CPM demonstrator will be used to validate the privacy use cases scenarios in WP4.

The WP3 works are split into 3 tasks:

- Task 3.1: Demonstrator specifications
- Task 3.2: Demonstrator development
- Task 3.3: Demonstrator functional test and validation

c) Planning T0+6 to T0+30

d) Deliverable:

- A CPM demonstrator

e) Expected results: This work package will deliver input for the WP4 activities.

WP3 Task 1	Title : Demonstrator specifications				
Start	T0+6	Duration	18 Months	Resources (m.m)	13
Partners		<u>INSIDE</u>	CEA-LETI	UVSQ	UPMF
Effort in m.m		3	3	6	1
Objectives : To specify the final project demonstrator					
Description of work:					
This task will address several goals:					
1) Identification of a relevant use case for demonstration					
2) Definition of the scenario of demonstration					
3) Definition of the hardware of the CPM demonstrator					
4) Definition of the software of the CPM demonstrator					
Selection of attack scenarios					
Goal : Validation of a subset of attack scenarios, selected according to the importance of the threat and the practical feasibility. This corresponds to the following two steps :					
- The study done in WP1 gives rise to several active and passive attack scenarios. The importance of the resulting threat may vary, together with the practical feasibility. It is important to select a small number of scenarios that represent the most threatening and realistic attacks.					



The definition of selection criteria for passive and active attack scenarios, and their respective weight in the decision making. (Cost of the attack, cost of the counter-measure, probability of occurrence, etc).			
Deliverable	Title	Date	Type
D 3.1.1	Demonstrator specifications	T0+24	Report
Validation criteria: Partners know how			

WP3 Task 2 Title : Demonstrator development					
Start	T0+6	Duration	24 Months	Resources (m.m)	30
Partners	INSIDE	CEA-LETI	UVSQ	UPMF	
Effort in m.m	14	16	0	0	
Objectives : To design and develop the final project demonstrator					
Description of work:					
This task will address several goals:					
1) Development of CPM demonstrator hardware in discrete components					
2) Development of a NFC device to be included into the CPM.					
3) Development of CPM demonstrator software					
4) Development of the specific software for the NFC device					
5) Development of use case and scenario simulator					
6) Development of test tools and test bench					
The demonstrator will propose embedded hardware and software solutions to address the main important targets related to those applications security needs. As the analysis at the system level security impact is not identified at this time, the demonstrator would probably have to propose solutions based on and not fully compliant with the published specifications. But, the product will have to be compliant with the security requirements.					
The demonstrator will be developed on a protocol level security evaluation, then it will be based on a device and a reader to provide a solution which could be reused at a system level.					
The demonstrator will provide example of functions related to real market needs / use case discussed by NFC forum as example of application.					
Deliverable	Title			Date	Type
D 3.2.1	Demonstrator hardware and software			T0+30	hardware
Validation criteria: Partners know how					

<b>WP3 Task 3 Title : Demonstrator test and validation</b>					
Start	T0+6	Duration	24 Months	Resources (m.m)	10
Partners	INSIDE	CEA-LETI	UVSQ	UPMF	
Effort in m.m	3	7	0	0	
Objectives : To design and develop the final project demonstrator					
Description of work:					

This task will address several goals:

1. Functional test of CPM demonstrator
2. Validation of CPM privacy functionalities
3. Technical conclusion

Based on the above specifications and applications, the demonstrator will propose solution to protect the user sensitive data, and provide options to answer the market needs and the deployment of significant amount of products.

Deliverable	Title	Date	Type
D 3.3.1	Test and experiments report	T0+30	Report
Validation criteria: Partners know how			

**WP4 : Security and privacy demonstration**

a) Objectives: The goal of this work package is to demonstrate the correctness and relevance of the CPM functionalities.

b) Description :

The validation work of the CPM is split into two parts:

- a) security issues
- b) privacy issues

The first point is to check if global and basic security of the contactless system is not affected by the new embedded privacy functions.

The second point is to assess the performance of the new embedded privacy functions with relevant use cases.

The WP4 works are split into 2 tasks:

- Task 4.1: Use case security demonstration
- Task 4.2: Use case privacy validation

c) Planning : T0+18 to T0+36

d) Deliverable :

- Demonstrations

e) Expected results:

Validation of the privacy primitives

WP4 Task 1	Title : Use case security demonstration				
Start	T0+18	Duration	12 Months	Resources (m.m)	4
Partners	INSIDE	CEA-LETI	UVSQ	UPMF	
Effort in m.m	1	3	0	0	
Objectives : To demonstrate a security use case					
Description of work:					
The main purpose of this task is to check that the new embedded privacy function do not weaken or jeopardize the basic security functions of a contactless system. This will be undertaken within the frame work of current and available security primitives.					
Deliverable	Title			Date	Type
D 4.1.1	Use case security demonstration			T0+30	Demo
Validation criteria: Demonstration relevance					

WP4 Task 2 Title : Use case privacy validation					
Start	T0+16	Duration	18 Months	Resources (m.m)	18
Partners	INSIDE		CEA-LETI	UVSQ	UPMF
Effort in m.m	1		2	6	9
Objectives : To design and develop the final project demonstrator					
Description of work:					
This task will validate the specific privacy functions of the CPM.					
1. Validation of each CPM privacy protection function					
2. Coherency, consistency and compatibility between the different privacy functions					
3. Coherency, consistency and compatibility with the security functions					
4. Test of the acceptance by users by the mean of the CAUTIC method Inquiry (User Aided Design for Technology, Innovation and Change)					
Security validation for the counter-measures					
Goal : Validation of counter-measures, from a security point of view					
Description of work :					
<ul style="list-style-type: none"><li>- Characterize the effectiveness of counter-measures</li><li>- Check that no side-effect limit the performances of the contactless system in nominal behavior (without attack)</li><li>- Propose an evaluation methodology for evaluating the security of the contactless interface</li><li>- Check consistency with related existing standards or on going standardization works</li><li>- Test and evaluate the user acceptability (usage attractors, conditions and inhibitors) and derive recommendations to support the finalization of the CPM applications.</li></ul>					
Deliverable	Title			Date	Type
D 4.2.1	Privacy protection demonstration			T0+36	Demo
D4.2.2	User and social acceptance			T0+36	Report
Validation criteria: Demonstration relevance					

**WP5 : project management**

a) Objectives: The main objective of this work package is to coordinate the work and the related partner's activities

b) Description:

The work package includes various activities:

- Project coordination
- Relations with ANR office
- Dissemination of results
- Confidentiality of results policy
- Consortium agreement
- Standardization activities

The work package WP5 is split into five tasks:

- Task 5.1: Project coordination
- Task 5.2: Dissemination of results

c) Planning: T0+0 to T0+36

d) Deliverable:

- Report on main technical results of the project
- Progress reports

e) Expected results:

- Good achievement of the project
- High level of collaboration between partners
- Valorization of the results

WP5 Task 1	Title : Project coordination				
Start	T0	Duration	36	Months	Resources (m.m)
Partners	INSIDE	CEA-LETI	UVSQ	UPMF	
Effort in m.m	0	3	0	0	
Objectives : To coordinate the project					
Description of work:					
The main purpose of this task is to coordinate the work according to the planning and between the partners. It will consist of:					
1) Organization of management meetings					
2) Organization of technical meetings					
3) Validation of deliverables					
4) Technical orientation and decision					
5) Relation with ANR					
6) Project review organization					

7) Confidentiality management			
Deliverable	Title	Date	Type
D 5.1.1	Yearly progress reports	T0+12 +24 & +36	Reports
Validation criteria: External audit and reviews			

WP5 Task 2 Title : Dissemination of results					
Start	T0+12	Duration	24 Months	Resources (m.m)	12
Partners		INSIDE	CEA-LETI	UVSQ	UPMF
Effort in m.m		1	3	6	2
Objectives : To disseminate the projects results through papers, seminar and web site					
Description of work:					
Description of work					
<ul style="list-style-type: none"><li>- Write papers describing the results and work of the project to International conferences or workshops to be identified (CHES, ...)</li><li>- Participation to congress (Cartes 200X)</li><li>- Validation of publications according to the confidentiality policy of the project</li><li>- Contribution to contactless PET standardization</li><li>- Workshops with consumers associations and public organizations involved in privacy</li></ul>					
Deliverable	Title			Date	Type
D 5.2.1	Papers, workshop, ....			T0+36	X
Validation criteria: Accepted papers, seminar organization					

### 1.6.3. Added value of collaboration

The consortium is well balanced with the presence of an SME involved in contactless products for secure applications, a public laboratory involved in applied research on contactless and secure electronic systems and an academic laboratory specialized in cryptography.

#### *INSIDE CONTACTLESS*

Inside Contactless will bring to the project COPRIM its expertise and know-how in design and manufacturing of secure contactless products. INSIDE will address both hardware and protocol aspects.

#### *CEA-LETI*

CEA-LETI will bring in the project its expertise in near field communication, contactless air interface design, secure specifications and electronic integration. LETI will mainly address the physical level and hardware implementation of the COPRIM project.

#### *UVSQ*

UVSQ will offer its well established competences in cryptography and secure protocol. UVSQ will address mainly the protocol development of the project

#### *UPMF*

UPMF will bring its large expertise in social sciences and basically in innovation and new technologies acceptance by end users (CAUTIC method – User Aided Design for Innovation, Technology and Change)

### 1.6.4. Management structure

The project coordination will be carried out at two levels:

- A Project Management Committee (PMC) with the project leader of each partner and possibly every WP leaders. One meeting every quarter.
- WP Technical Committees (WPTC) managed by the WP leader. Technical meetings will be scheduled according to the requirements, but at least one every quarter. Basically they will be scheduled at the same date and place than the PMC.

PMC will have the role of an administrative and technical steering committee. It will address the planning of the consortium meetings, deliverables to ANR, dissemination of information and publication control. PMC will have in charge to set the consortium agreement at the beginning of the project.

### 1.6.5. Risks assessment

#### Risk management:

Technical risks will be raised up and presented by the WPTC leaders to the PMC. The role of the PMC will be to propose a solution and decide the action plan.

### 1.6.6. Main milestones and deliverables

Milestones	Date	Deliverables	Coord.	Task
<b>Year 1</b>				
M1	T0+12	D 1.1.1 Scenarios and uses cases report	UPMF	WP 1.1
M1	T0+12	D 1.2.1 Analysis report	CEA-LETI	WP 1.2
M1	T0+12	D 1.3.1 CPM Specification report	INSIDE	WP 1.3
M1	T0+12	D 5.1.1 Year 1 progress report	CEA-LETI	WP 5.1
<b>Year 2</b>				
M2a	T0+24	D 2.1.1 Sensing and jamming functions report	CEA-LETI	WP 2.1
M2a	T0+24	D 2.2.1 Protection at protocol level report	UVSQ	WP 2.2
M2a	T0+24	D 2.3.1 Report on cross-layer optimization	INSIDE	WP 2.3
M2a	T0+24	D 3.1.1 Demonstrator specifications	INSIDE	WP 3.1
M2a	T0+24	D 5.1.2 Year 2 progress report	CEA-LETI	WP 5.1
<b>Year 3</b>				
M2b	T0+30	D 3.2.1 Demonstrator hardware and software	CEA-LETI	WP 3.2
M2b	T0+30	D 3.3.1 Test and experiments report	CEA-LETI	WP 3.3
M2b	T0+30	D 4.1.1 Use case security demonstration	CEA-LETI	WP 4.1
M3	T0+36	D 4.2.1 Privacy protection demonstration	INSIDE	WP 4.2
M3	T0+36	D 4.2.2 User and social acceptance	UPMF	WP 4.2
M3	T0+36	D 5.2.1 Dissemination report	UVSQ	WP 5.2
M3	T0+36	D 5.1.3 Year 3 progress report	CEA-LETI	WP 5.1

### 1.6.7. Main project reviews



An external project review will be planned every year with the ANR representative.

Internal project review will be done at each PMC meeting every quarter.

### 1.6.8. Planning of work packages and tasks

	Year 1				Year 2				Year 3			
<b>WP1</b>												
T1.1 Personal data and privacy use cases												
T1.2 CPM and threats analysis												
T1.3 CPM specifications												
<b>WP2</b>												
T2.1 Design of protection at physical level												
T2.2 Design of protection at protocol level												
T2.3 Cross layer design												
<b>WP3</b>												
T3.1 Demonstrator specifications												
T3.2 Demonstrator development												
T3.3 Demonstrator test and validation												
<b>WP4</b>												
T4.1 Use case security demonstration												
T4.2 Use case privacy validation												
<b>WP5</b>												
T5.1 Project coordination												
T5.2 Results dissemination												
<b>Main Milestones</b>												
1- CPM specification												
2- Design completed												
3- Demonstration												

## 1.6.9. Manpower resources per task and per partners

Resources Breakdown								
Task	Description	Leader		INSIDE	LETI	UVSQ	UPMF	TOTAL
T1.1	Personal data and privacy use cases	UVSQ	Y 1	2	2	6	5	16
			Y 2					0
			Y 3					0
			Total	2	2	6	5	16
T1.2	CPM and threats analysis	LETI	Y 1	3	4	6	1	14
			Y 2					0
			Y 3					0
			Total	3	4	6	1	14
T1.3	CPM specifications	INSIDE	Y 1	3	4	0	0	7
			Y 2					0
			Y 3					0
			Total	3	4	0	0	7
WP1	Privacy threats analysis		Y 1	8	10	12	8	38
			Y 2	0	0	0	0	0
			Y 3	0	0	0	0	0
			Total	8	10	12	8	38
T2.1	Design of protection at physical level	LETI	Y 1	4	3			7
			Y 2	8	7			16
			Y 3					0
			Total	12	10	0	0	22
T2.2	Design of protection at protocol level	UVSQ	Y 1		1			1
			Y 2	1	1	6		8
			Y 3					0
			Total	1	2	6	0	9
T2.3	Cross layer design	INSIDE	Y 1		1			1
			Y 2	1	3			4
			Y 3					0
			Total	1	4	0	0	6
WP2	CPM Design		Y 1	4	6	0	0	9
			Y 2	10	11	6	0	27
			Y 3	0	0	0	0	0
			Total	14	18	6	0	38
T3.1	Demonstrator specifications	INSIDE	Y 1	1	1		1	3
			Y 2	2	2	3		7
			Y 3			3		3

			Total	3	3	6	1	13
			Y 1	2	3			5
			Y 2	6	7			13
			Y 3	6	6			12
T3.2	Demonstrator development	LETI	Total	14	16	0	0	30
			Y 1		1			1
			Y 2	1	2			3
			Y 3	2	4			6
T3.3	Demonstrator test and validation	INSIDE	Total	3	7	0	0	10
			Y 1	3	6	0	1	9
			Y 2	9	11	3	0	23
			Y 3	8	10	3	0	21
WP3	CPM Development		Total	20	28	6	1	55
			Y 1					0
			Y 2		1			1
			Y 3	1	2			3
T4.1	Use case security demonstration	LETI	Total	1	3	0	0	4
			Y 1					0
			Y 2		1	2		3
			Y 3	1	2	4	9	16
T4.2	Use case privacy validation	INSIDE	Total	1	3	6	9	19
			Y 1	0	0	0	0	0
			Y 2	0	2	2	0	4
			Y 3	2	4	4	8	18
WP4	Security and Privacy Demonstration		Total	2	6	6	8	22
			Y 1		1			1
			Y 2		1			1
			Y 3		1			1
T5.1	Project coordination	LETI	Total	0	3	0	0	3
			Y 1		1	2		3
			Y 2		1	2		3
			Y 3	1	1	2	2	6
T5.2	Results dissemination	UVSQ	Total	1	3	6	2	12
			Y 1	0	2	2	0	4
			Y 2	0	2	2	0	4
			Y 3	1	2	2	2	7
WP5	Project Management		Total	1	6	6	2	15
<b>TOTAL</b>			<b>Total</b>	<b>46</b>	<b>84</b>	<b>38</b>	<b>18</b>	<b>183</b>
				<b>INSIDE</b>	<b>LETI</b>	<b>UVSQ</b>	<b>UPMF</b>	<b>TOTAL</b>

### 1.7. Expected results and perspectives

#### 1.7.1. Project objectives & expected outcome with evaluation criteria for success measurement

##### Scientific outcome

- Mid field modeling and characterization (+Near and Far)
- Privacy proof PHY layer (with low cost and standard compliance approach)
- Privacy proof Protocol layer (with low cost and standard compliance approach)

##### Technical outcome

- Privacy management demonstrator
- Handheld and autonomous portable device demonstrator
- Feasibility of device and embedded functions

##### Industrial outcome

- Privacy portable prototype
- Trust and confidence for users
- Contactless Privacy Enhancing Technology standards

##### Economical outcome

- Manufacturing and distribution of CPM devices
- Increase of contactless markets (new and enlarge)

##### Societal outcome

- Privacy management
- Privacy devices access for citizens and consumers
- Confidence in portable privacy device
- Confidence in ambient Intelligence
- Validation of end users acceptance

##### Evaluation criteria

Expected outcome	Success criteria
Scientific outcome	
EM Mid field modeling	Experimental validation
Secure PHY layer	Efficiency with low cost implementation
Secure PRO layer	Efficiency and low computing resource requirements

Technical outcome	
Privacy management demonstrator	Technico-economic trade off Effectiveness of privacy functions validated via experiments
Handheld and autonomous portable device demonstrator	Technico-economic trade off
Feasibility of device and embedded functions	Technico-economic trade off
Industrial and economical outcome	
Privacy portable prototype	Low cost device
Trust and confidence for users	Validation CAUTIC method criteria Consumers acceptance
Manufacturing and distribution of CPM devices	Cheap devices New distribution circuits separate from services providers
Increase of contactless markets (new and enlarge)	Sales volumes
Standardizations	
Standardization proposal	Acceptance within standardization committees of technical proposals
Other outcome	

### 1.7.2. Scientific and applications perspectives

#### Scientific/technical perspectives

- a) New scheme of privacy control
  - a. At technical levels
  - b. At user level
- b) Coherency and convergence of different approaches

#### Applications

- a) Citizen level
  - a. E-government documents
  - b. E-citizen cards
- b) Consumers
  - a. RFID deployment
  - b. Ambient intelligence

**Industrial**

- a) Manufacturing of CPM
- b) Distribution of CPM
- c) Standardization (of RFID devices and CPM)

**1.7.3. Relation with existing standards**

The works carried out in the project will be in close connection with ISO SC17 and SC31, but also with NFC Forum.  
Inside Contactless is member of NFC Forum.

Inside Contactless and CEA-LETI are members of ISO/AFNOR in SC17 (Smart cards) and SC31 (RFID tags) committees.

The project will follow the works done at the European Expert Group on RFID.

**1.8. Intellectual property**

The partners of the COPRIM project agree on the following intellectual property principles statements.

**Definitions**

**PRIOR KNOWLEDGE:** any knowledge, patented or not, know-how, secret trade or any other type of information in some form that it is, pertaining to a Party or held by it before the date of signature of the AGREEMENT or developed or acquired by it in parallel with the execution of the AGREEMENT, but necessary to the execution of the PROGRAM or the exploitation of NEW KNOWLEDGE.

**NEW KNOWLEDGE:** any knowledge patented or not, know-how, secret trade or any other type of information, in some form that it is, resulting directly from work of the PROGRAM carried out by the Parties within the framework of the AGREEMENT.

**Intellectual property**

1/ Each Party remains the owner of its PRIOR KNOWLEDGE.

However, for the needs for the execution of the PROGRAM and for this only purpose, each Party will be able to use without financial counterpart, PRIOR KNOWLEDGE of another Party. This PRIOR KNOWLEDGE will be communicated by the holder Party on request express of another Party and will have to be treated like confidential information.

2/ Each Party will be owner of the NEW KNOWLEDGE obtained by its personnel without the contest of the personnel of another Party pursuant to the work of the PROGRAM undertaken by it (hereafter, INDIVIDUAL NEW KNOWLEDGE). The possible subsequent patents will be deposited with its name and at its own expenses

3/ The NEW KNOWLEDGE obtained jointly by the personnel of several Parties pursuant to work undertaken in common tasks of these Parties (hereafter, JOINT NEW KNOWLEDGE) will be said being the common property of the concerned Parties and the possible subsequent patent applications will be deposited with their joint names and at their divided expenses. These deposits will mention the names of the researchers and/or engineers concerned. The concerned Parties will work out a payment of joint ownership of the patents concerned before any exploitation.

#### Exploitation principles

##### 1/ Exploitation of PRIOR KNOWLEDGE

Each Party has its PRIOR KNOWLEDGE freely.

Each Party is committed conceding with the other Parties, on request express of those, and subject to the rights of the third parties, licenses on its PRIOR KNOWLEDGE necessary to the valorization of NEW KNOWLEDGE of the other Parties to normal commercial conditions for the sector of application considered.

##### 2/ Exploitation of NEW KNOWLEDGE

a/ Each Part has will be able freely to use and directly exploit its INDIVIDUAL NEW KNOWLEDGE or by way of grant of licenses.

b/ The joint owners Parties of JOINT NEW KNOWLEDGE will set up their methods of exploitation under regulation of joint ownership agreement.

c/ NEW KNOWLEDGE of a Party which would be necessary to the exploitation of NEW KNOWLEDGE of another Party will be the subject of a license, subject to the rights of the third Parties and normal commercial conditions, to be negotiated between the concerned Parties before any exploitation.

A consortium agreement (CA) will be set up by the partners at the beginning of the project.



## 2. Financial resources

### 2.1.1. Manpower and budget

Partners	Man months breakdown					Total m.m	Total Budget	Requested Funding
	WP1	WP2	WP3	WP4	WP5			
INSIDE	8	14	20	2	1	45	660 k€	397 k€
CEA-LETI	10	14	26	6	6	64	834 k€	417 k€
UVSQ	12	6	6	6	6	36	245 k€	104 k€
UPMF	6	0	1	9	2	18	104 k€	58 k€
Total	36	38	55	23	15	167	1843 k€	976 k€

### 2.1.2. Justification of personnel, equipments, traveling, operating costs

Partners	Expenditures (€)					Permanent (h)	Temporary (h)	Total hours
	R&D equipments	Consumables	Travel	Internal	Sub- contracting			
INSIDE	28200	12000	7000	0	12000	7605		7605
CEA-LETI	36000	20000	8500	0	32000	8693		8693
UVSQ	5000	5500	5500	0	0	4866	1632	6498
UPMF	0	2200	2000	0	0	1020	2400	3420
Total	69200	39700	23000	0	44000	22184	4032	26216

#### Manpower:

The manpower involved in the project will basically consist of electronic hardware and software engineers and cryptographic researchers.

**Equipments:**

- This project does not require any specific equipment.
- Work stations and PC.
- Standard instrumentations such as scopes, wave generators, power supply and spectrum analyzer will be used.
- Integrated component will be developed with CAD tool for the design.
- Sub-contacting will be used for electronic boards and chip design and/or manufacturing.
- Instrumentation will be used for the development and the validation of the works.

**2.1.3. Other public funding of the project**

There is no other public funding that is related to the COPRIM project.

## **Annexe 5. Les trois temps du travail de scénarisation**

Cette annexe est consacrée au récit du travail de scénarisation dans le projet. Ce compte-rendu, qui a servi de point d'appui à l'analyse, en constitue déjà un commencement. Ainsi, il n'engage aucune volonté d'objectivation « pure » du déroulement des événements mais porte les stigmates de l'analyse approfondie qui lui succède. Sa structuration en trois parties en est dépendante et elle permet d'appréhender le chemin parcouru par le scénario avant qu'il ne devienne un « tremplin », un « container à idées<sup>1</sup> ». Nous espérons ainsi que la possible impression d'incomplétude qui peut survenir à la lecture de ces lignes soit dissipée à la lumière du reste de l'analyse. Aussi, ce choix de présentation est justifié par l'intensité technique du travail de projection d'usage : rendre compte du travail de scénarisation dans un environnement de conception implique de rendre compte d'actes et de procédures techniques parfois complexes et dont l'évocation n'est familière que pour un groupe d'initiés.

Le stade préliminaire de la scénarisation (a) est celui d'une mise en accord sur la « sécurité » comme problème essentiel et commun à l'ensemble de l'équipe-projet. Durant ce premier temps, on observe une « stabilisation<sup>2</sup> » de l'intrigue autour de cette question sans pour autant que l'ensemble des participants aux scénarios soit clairement défini. Le scénario n'a alors de matérialisation qu'idéelle. Dans un second temps (b), c'est le corps du scénario qui va se stabiliser autour d'éléments narratifs et de procédures technologiques descriptives. L'accent est alors mis sur l'articulation de l'intrigue et de son environnement. Enfin, les scénarios vont devenir des lieux de représentation à la nature hybride (c) oscillant entre « task-driven stories » et « human-centered stories », description et prescription, exploration et évaluation. Les scénarios sont alors un patchwork de représentations qui obéissent à différents objectifs de l'activité de conception (Bodker 1998). Nous souhaitons montrer que ce travail s'effectue dans un double mouvement : d'une part, les incertitudes propres à l'écologie socio-technique sont réduites et stabilisées (a et b) ; d'autre part, cette première

---

<sup>1</sup> «Creating something new is not a matter of deriving from the existing. However, the view that representations are containers of ideas means that there is less of a difference between the new and the present, because it is not a matter of mapping but of containing ideas.» Susanne Bodker, 'Understanding Representation in Design', *Hum.-Comput. Interact.*, 13/2 (1998), 107-25.

<sup>2</sup> «The degree of stabilization was introduced as a measure of the acceptance of an artifact by a relevant social group. The more homogeneous the meanings attributed to the artifact, the higher is the degree of stabilization. [...] These stabilization processes have a dual character: They include irreversible processes of closure that impose a steplike character onto technical change, but they are also continuous in-between, as is described by growing and diminishing degrees of stabilization.» Trevor Pinch, 'Do Not Despair: There Is Life after Constructivism', *Science, Technology & Human Values*, 18/1 (1993a), 113-38 at 121.

étape, rouvrir les champs du possible en s'appuyant sur les éléments stabilisés pour construire les fictions (c).

## ***A - La stabilisation de l'intrigue : le problème technologique comme consensus***

Au départ, le scénario, bien qu'encore à l'état de concept, comprend une multitude de formes d'existence de l'utilisateur. L'humain est alors un attaquant, un utilisateur, un client, compris comme agissant de manière rationnelle (motivations économiques) ou « pour le fun » (chef de projet). C'est une entité floue. Tandis que sa définition formelle ne constitue pas alors une priorité, l'intrigue qui doit s'inscrire au cœur du scénario est dictée par l'impératif de répondre à la sécurisation de l'information échangée. Le scénario doit impérativement mettre en scène des « menaces », « attaques » et « parades » du système d'information, toutes devant faire l'objet d'une évaluation comparative.

Ainsi, l'on peut distinguer deux sources distinctes qui nourrissent le scénario. D'une part, l'intrigue s'organise à partir d'une lecture technologique de la sécurité de l'information. D'autre part, l'autre source d'information est constituée par l'environnement au sein duquel se déroule l'intrigue. Cette scission des sources de création du scénario participe du caractère déjà hybride de celui-ci : tandis qu'une dose de créativité *extrascientifique* semble autorisée pour l'élaboration de l'environnement, cette créativité est bornée par l'intrigue au cœur des scénarios. Le scénario est d'abord un lieu où se joue la résolution d'une « menace » pesant sur la sécurité de l'information. Il appartient alors aux représentants des usagers de renseigner le consortium sur les règles du jeu en vigueur dans l'environnement de cette « menace ». Cependant, la caractérisation de la menace va rejaillir de manière inattendue sur la nature et la fonction originellement prévues pour le scénario.

### **a) Comité de pilotage 1 (T0)**

Participants : CEA-LETI (3), UMANLAB (3), UVSQ (1), INSIDE (1 – entretien téléphonique), ANR (1)<sup>1</sup>

---

<sup>1</sup> Entre parenthèses figurant le nombre de participants à l'évènement. Le cas échéant, la participation par le biais téléphonique est indiquée. Les moments d'intervention des réunions sont indiqués par un T et par un chiffre associé indiquant la distance en mois avec le début du projet indiquée en T0.

La matinée a permis aux partenaires de faire connaissance entre eux (tour de table de présentation de dix minutes par partenaire), d'introduire le projet dans son ensemble (CEA-LETI) et de rappeler les contributions prévues pour chaque partenaire. L'après-midi était consacrée au règlement des aspects administratifs et organisationnels du projet et à la finalisation des modalités de lancement des travaux (WP 1 et WP 2). Il faut noter la présence d'une représentante de l'ANR à la réunion.

Ni les présentations des partenaires, ni celle du projet n'ont été suivies de questions ni de discussions de la part des auditeurs. En revanche, le moment consacré à la présentation des contributions respectives a déclenché plusieurs réactions du CEA-LETI suite aux présentations de Umanlab et d'Inside. Le CEA-LETI a précisé le rôle de Umanlab en exprimant le souhait que leur contribution puisse favoriser la distinction entre « peurs réelles et peurs infondées ». Le chef de projet dit avoir entendu parler de modèle quantitativiste d'acceptabilité de l'innovation par les utilisateurs et nous enjoint à nous en inspirer. Cette précision établie est confirmée par la précision apportée au rôle d'Inside : « apporter des scénarios sur lesquels les clients ont des réticences ou des inquiétudes ». De même, suite à une question d'un sociologue, le CEA-LETI a donné une définition succincte des scénarios comme un « ensemble de menaces, de moyens à mettre en œuvre pour l'attaque et de coût de la protection à mettre en œuvre », la combinaison des trois permettant de jauger la pertinence des scénarios à choisir. Une longue discussion s'engage autour de la question des scénarios. Aussi, le rôle des institutions judiciaires (droit européen) ou normatives (CNIL) est discuté concernant la protection de la « Privacy ». Par ailleurs, Inside a également évoqué l'absence de modèle économique pour le mode « peer-to-peer<sup>1</sup> ».

Lors de cette réunion, il est acté qu'un rapport d'avancement doit être remis à l'ANR chaque semestre par le consortium et qu'à mi-parcours (T0+15) les travaux devront faire l'objet d'une présentation devant un comité d'experts réunis par l'ANR. Un accord est alors établi entre les partenaires pour fixer trimestriellement la fréquence des réunions « en face-à-face » sans exclure l'opportunité d'échanges informels entre ces moments de rencontre.

L'organisation du WP 1 est rappelée comme étant marquée par la livraison d'un rapport incluant trois parties :

---

<sup>1</sup> Voir chapitre 4.

- II. Un état de l'art des menaces potentielles contre la « Privacy » spécifiques au sans contact<sup>1</sup>
- III. Un état de l'art des protections technologiques disponibles
- IV. Des scénarios d'usages et des spécifications à adresser dans le projet<sup>2</sup>. L'objectif des spécifications est double : d'une part, identifier les fonctionnalités idéales que devrait recouvrir un Contactless Privacy Manager (CPM) ; d'autre part, sélectionner l'éventail des fonctionnalités qui seront retenues dans le projet.

Le travail est subdivisé en trois tâches :

- V. Scénarios d'usage autour de la notion de « Privacy »
- VI. Analyse des dispositifs sans contact et des menaces attachées
- VII. Spécifications finales des fonctions sélectionnées pour le CPM

Les résultats issus de ce premier workpackage doivent alimenter les WP2 2, WP 3 et WP 4. Enfin, le document qui sert de référence au consortium, l'annexe technique, est porté à connaissance de l'équipe Umanlab.

#### **a) Réunions internes**

Durant les réunions internes intercalées entre les deux premiers comités de pilotage, nous avons pris conscience des difficultés que nous avions à cerner clairement les objectifs du projet. Tant le rôle attendu du CPM que plus largement le fonctionnement de la technologie NFC nous échappaient et compliquaient relativement l'entame d'un travail sur l'état de l'art de la notion de « Privacy », en particulier dans ses liens avec le sans contact.

#### **b) Comité de pilotage 2 (T0+3)**

Participants : CEA-LETI (3), UMANLAB (3), UVSQ (1), INSIDE (1, différent du participant initial)

La matinée était consacrée à l'état d'avancement de chacun des partenaires sur les états de l'art. Durant l'après-midi, les critères de sélection des scénarios pertinents devaient être ébauchés.

Umanlab a entamé par une présentation en deux temps en affirmant sa volonté de se saisir des menaces pour en faire des scénarios d'usage. En premier lieu, a été exposé aux

---

<sup>1</sup> Voir annexe 2.

<sup>2</sup> Voir annexe 3.



partenaires un ensemble de transparents reprenant dans les grandes lignes le fonctionnement du NFC avec l'objectif avoué d'être assuré d'une bonne compréhension de celui-ci. Dans un second temps, à partir d'une définition de la « Privacy » empruntée au HCI<sup>1</sup>, les sociologues ont insisté sur le caractère multifactoriel de la notion<sup>2</sup>. Enfin, la présentation s'est achevée sur une série de trois interrogations concernant le périmètre d'action du CPM<sup>3</sup>, la nature des menaces prises en compte dans le projet, et enfin les différentes appréciations des partenaires de la notion de « Privacy ». L'équipe-projet a décidé d'attendre la fin du tour de présentations pour répondre aux questions posées, en supposant que les travaux des autres partenaires contiendraient des réponses satisfaisantes. Cependant, Umanlab a insisté sur un point particulier : l'équipe voulait obtenir confirmation de la non-intégration du CPM au téléphone mobile comme préconisé dans l'annexe technique<sup>4</sup>. En effet, elle a exprimé ses réserves sur le fait d'avoir à entamer le travail de scénarisation sans aucune idée de l'aspect du CPM. Lorsque Umanlab a évoqué la possibilité d'explorer des pistes de développement technologique non réalisables immédiatement, le CEA-LETI a fait état de sa réticence « faire du travail pour rien ».

La présentation suivante a été l'œuvre du CEA-LETI. L'inventaire des familles d'attaques étudiées figurait dans la première partie de la présentation : un tableau à double entrée a été proposé comme moyen de classement des attaques et des contremesures<sup>5</sup>. En lignes, figuraient les attaques et en colonnes, les risques associés (risques, coût de l'attaque, scénarios possibles, standards impliqués, contremesures, coût des contremesures). Le chef de projet a fait la distinction entre des attaques économiquement motivées, les attaques « pour le fun » ou encore celles visant à démontrer ses compétences dans les communautés de piratage

---

<sup>1</sup> « The Privacy space is broken down into a set of interdependent dimensions that help defining phenomenon's implications for Privacy. These dimensions are interdependent and flexible. They are system properties, actor relations and information types. » Scott Lederer, 'Designing Disclosure: Interactive Personal Privacy at the Dawn of Ubiquitous Computing', (University of California 2003a).

<sup>2</sup> Voir annexe 1, figures 3 et 4.

<sup>3</sup> Notons qu'à l'évocation du dispositif par les sociologues sous le nom « COPRIM », le chef de projet a corrigé en insistant sur le fait que le nom du démonstrateur était le CPM.

<sup>4</sup> « Moreover, to increase trust and confidence of the user, it seems very relevant that this device must be a stand-alone one, fully controlled by the user. It must be its own and personal security resource for contactless devices management, in particular because of potentially unauthorized and covert remote hostile activation. » (annexe 4)

<sup>5</sup> Voir figure 2 de l'annexe 1.

électronique. Dès lors, un membre de Umanlab a considéré l'existence de deux types d'utilisateurs des dispositifs : l'attaquant et l'utilisateur légitime. Le chef de projet a considéré qu'il ne fallait pas négliger un troisième utilisateur, l'opérateur susceptible d'être lésé en cas d'attaque réussie quelque soit son domaine d'activité (banque, médical, politique, services, téléphonie, transport). Un court deuxième temps a été consacré à la présentation de solutions déjà existantes. Enfin, une proposition de fonctionnalités du CPM a été présentée, celui-ci n'étant alors intégré dans aucun dispositif technologique<sup>1</sup>. Celui-ci est présenté comme un brouilleur empêchant des lecteurs non autorisés de lire des tags portés par l'utilisateur. Le chef de projet s'interroge sur l'identité même de l'objet : doit-il être « stand-alone » ou intégré au tag ? Une discussion s'est alors engagée entre Inside et le CEA-LETI sur le vocabulaire utilisé lors de cette présentation durant laquelle le CEA-LETI a indistinctement utilisé les termes « cartes sans contact », « tags », « tags RFID » pour désigner le NFC. Pour Inside, le NFC brouille des catégories qui se distinguaient notamment par une séparation entre identification des personnes (contactless card) et traçage des objets (RFID) : « Le NFC est venu fausser cela et rapprocher les mondes » (Inside). Durant cette discussion, le CEA-LETI a précisé que le CPM était d'ores et déjà en cours de développement avancé. C'est un boîtier électronique qui « n'a rien de portable ». Il restait à l'adapter aux spécificités du NFC : « Le travail à faire dans COPRIM, c'est adapter le CPM au 13.56 [mhz], le NFC, quoi ! » En anticipant l'écriture des scénarios, Umanlab a proposé d'imaginer deux versions de scénario selon le choix d'intégrer ou pas le CPM à un dispositif existant avant qu'une discussion se soit engagée sur la portée de protection du CPM.

La présentation de l'UVSQ, à l'inverse des deux précédentes, s'est effectuée sur tableau blanc. Le cryptologue a repris les objectifs clés de la sécurité en cryptographie, soit le fait d'assurer la confidentialité, l'authenticité et l'intégrité des informations protégées. Le cryptologue a présenté les trois entités usuellement utilisées en cryptologie : « Alice » et « Bob » représentant les deux entités désirant échanger de l'information et « Charlie » est le nom attribué à l'attaquant. En réponse à la question de Umanlab, le cryptologue a affirmé « qu'en tant que telle, la notion de Privacy n'existe pas en cryptologie ». En complétant, le CEA-LETI a assuré que « l'idée qui traîne est que la sécurité s'oppose à la Privacy. » Plusieurs exemples « sociaux » sont mobilisés en illustration des présentations du

---

<sup>1</sup> Voir figure 1 de l'annexe 1.

cryptologue : les cartes « Myfair » de Philips, les algorithmes des GSM, les télécommandes de voitures à distance, les PDA, les passeports électroniques.

L'intervention d'Inside s'est effectuée par téléphone en début d'après-midi. L'interlocuteur s'est excusé de n'avoir pu préparer la réunion : il a remplacé au pied-levé l'interlocuteur précédent qui a alors quitté l'entreprise. Inside s'est présentée comme spécialiste du NFC et participant au NFC forum<sup>1</sup>. Inside a présenté son « cœur de métier » comme étant la conception et la vente de puces à des clients divers tels que des industriels intégrateurs de solution, des fournisseurs de téléphones, des opérateurs GSM, des fondeurs, des encarteurs. En réponse aux questions posées par Umanlab, Inside a présenté les scénarios d'attaque comme étant répartis par domaines d'activité (banque, assurance, santé, sécurité) bien que certaines attaques soient communes à plusieurs domaines. Par « use case » est entendue la mise en situation du NFC : « smart poster », « peer-to-peer », « contactless token ». Une histoire de la carte à puce est également offerte « de la puce simple à la puce à microprocesseur jusqu'à la puce capable de dialoguer comme un lecteur ». Inside a enfin précisé que « ce qu'il manque aujourd'hui pour le NFC, ce sont les applications. Aucun fournisseur ne propose encore de services en masse mais il y a quelques exemples pilotes dans les transports. Les opérateurs poussent autant que les fournisseurs de téléphones. » Le chef de projet a complété l'intervention en affirmant qu'à terme, le but était néanmoins l'interactivité totale entre dispositifs intégrant des tags NFC : ordinateurs, imprimantes, appareils photos. Durant cette présentation, de nombreux échanges ont lieu entre le CEA-LETI et Inside sur des aspects techniques de la technologie et notamment sur le fait que l'emploi de vocabulaires différents par les deux parties soit dû au processus de standardisation toujours en cours.

L'après-midi a été consacrée à ébaucher tous ensemble une définition des scénarios et des critères d'évaluation de ceux-ci. Un brainstorming collectif s'est mis en place pour compléter la grille amorcée par le CEA-LETI qui a d'ailleurs souligné l'importance « d'avoir un aspect malveillant à l'origine du scénario afin de ne pas aborder les problèmes relevant simplement du fonctionnement du dispositif. »

---

<sup>1</sup> Association de standardisation des normes du NFC, voir chapitre 4.

### c) Réunions internes (T0+ 3/4)

En parallèle du travail sur l'état de l'art, Umanlab éprouvait de grandes difficultés à entrevoir des ébauches d'attaques de communications NFC et surtout le rôle précis que le CPM pouvait jouer pour l'utilisateur. Durant les séances, des exemples ont été imaginés à partir d'expériences personnelles : valider son forfait de ski avec une carte NFC, payer le parking, etc. Malheureusement, il nous était difficile de saisir les motivations de l'attaque et de trouver de la vraisemblance dans les situations décrites. Le choix a donc été fait de solliciter le CEA-LETI, partenaire le plus proche géographiquement, pour obtenir des précisions sur les conditions de réalisation des attaques.

Aussi, le découpage entre plusieurs pôles de réflexion a été précisé : bien qu'ils étaient liés entre eux, nous avons choisi de distinguer dans la réflexion les scénarios d'usage, des scénarios d'attaque et du concept de « Privacy ». C'est dans ce contexte qu'a émergée l'idée de s'emparer dans notre travail de certains éléments terminologiques ou conceptuels présentés par nos partenaires. Ainsi, pour mieux comprendre les scénarios d'attaque, nous avons mis en scène « Alice », « Bob » et « Charlie », chacun de nous jouant le rôle de l'un deux au sein de ce que nous nommions des *configurations d'usages*. Celles-ci étaient caractérisées par trois éléments : les acteurs présents, le type d'interaction entre eux et les enjeux de l'interaction. Ces configurations s'inscrivaient dans des domaines d'application que nous explorions au fil de nos improvisations et inspirées des comptes-rendus évoqués dans la littérature grise. La notion de « Privacy » intervenait, à ce moment, comme celle à partir de laquelle ces configurations devaient être interrogées. Cependant, nous éprouvions encore des difficultés à caractériser cette notion au vu du faible avancement de l'état de l'art et de sa relative équivocité lorsqu'évoqué par les partenaires. Enfin, une matrice résumant l'ensemble de ces réflexions à vu jour peu à peu. Il s'agissait d'un tableau à double entrée reprenant en colonne les scénarios d'attaque et en ligne les domaines d'application<sup>1</sup>. Nous considérions ainsi que chaque « case » de cette matrice correspondait à une configuration d'usage particulière à analyser avec un concept stabilisé de « Privacy ». Le responsable projet a noté que cette matrice pouvait servir d'outil de médiation puissant entre l'ensemble des partenaires, si ceux-ci en percevaient l'utilité. Devant cet espoir, nous avons décidé de profiter de la proximité géographique avec le CEA-LETI, afin d'organiser une réunion pour « faire le point ». Enfin,

---

<sup>1</sup> Voir annexe 1, figure 5.

le chargé de recherche s'est inquiété de la vitesse d'avancement du travail. Le responsable projet lui a répondu que deux cadences existaient : une cadence de travail interne caractérisée par des réunions régulières avec pour objectif l'exploration des possibilités de valorisation académique et une cadence de travail externe rythmée par les dates de livraison des livrables et sur laquelle nous ne devions pas influencer.

#### **d) Réunion CEA-LETI/Umanlab (T0 + 4)**

Lors de la réunion avec l'un des membres du CEA-LETI, celui-ci a présenté l'attaque en relais comme celle sur laquelle les scénarios devaient se concentrer. La priorité, pour le projet, était d'aboutir à l'évaluation des risques. Après avoir fait l'effort de nous expliquer chacune des attaques en des termes plus accessibles, moins techniques, notre interlocuteur a admis considérer que les aspects sociaux, économiques et légaux en lien avec la problématique lui étaient complètement étrangers. Dès lors, il ne pouvait apporter son conseil qu'en vertu de critères techniques. Enfin, une discussion s'est engagée pour savoir en quoi consistait la sociologie et quelles méthodes stables et scientifiques arrivions-nous à développer pour faire de la science.

#### **e) Réunion interne (T0 + 5)**

Nous travaillions toujours sur l'état de l'art afin d'aboutir le plus rapidement possible à une appréciation solide de la notion de « Privacy ». Ce travail s'orientait de plus en plus sur trois pistes : les notions de risque, de confiance et de « Privacy », que nous traduisions souvent en français par vie privée<sup>1</sup>. Nous avons également décidé de rechercher dans la littérature spécialisée sur le NFC des cas d'expérimentation de la technologie NFC comme moyen d'inspiration pour l'élaboration des scénarios. Enfin, nous nous sommes fixés comme objectif de proposer des ébauches de scénarios pour le prochain comité de pilotage. Nous souhaitions également nous y rendre en ayant stabilisé les concepts clés de notre état de l'art.

#### **f) L'évènement déstabilisateur (T0 + 5 ½)**

Nous avons été surpris et décontenancés par la réception d'un mail provenant du CEA-LETI :

---

<sup>1</sup> Les trois notions sont citées dans l'annexe technique/annexe 4.

« J'aimerais que l'on se rencontre entre voisins pour faire un point sur les différents scénarios induisant des problèmes de Privacy avant le prochain COPIL et la conf call. En particulier, il serait bien de déterminer dans chacun de nos scénarios une échelle de dangerosité (si c'est possible, à discuter !)... une sorte de mesure de la perte de Privacy. »

Membre du CEA-LETI

Jusqu'ici, nous avons envisagé que la rédaction des scénarios prendrait appui sur les conclusions des états de l'art. Or, nous comprenions à ce moment que le CEA-LETI désirait que ceux-ci soient prêts le plus rapidement possible et pensait que nous avions les moyens et compétences de les produire dans des délais brefs. Par ailleurs, nous considérons ne pas être en possession d'informations suffisantes pour avancer ; nous éprouvons particulièrement le besoin d'obtenir d'Inside des informations sur l'état actuel du marché et les applications existantes. Nous avons donc réagi à ce mail par l'organisation d'une nouvelle réunion entre le CEA-LETI et nous pour clarifier ces divergences de vue.

#### **g) Réunion CEA-LETI/ Umanlab (T0 + 6)**

La réunion a donc débuté par un bref rappel des objectifs du projet et du workpackage 1. Ce bref détour nous a notamment permis de souligner la distribution des rôles tels que spécifiés dans l'annexe technique. Il s'agissait moins de délimiter les rôles propres de chacun des partenaires que de souligner la précocité de la demande formulée par le CEA. Cependant, nous avons profité de cette introduction pour évoquer la nécessité d'une participation des partenaires « techniques » à l'élaboration des scénarios. Or, ce qui relevait de l'évidence, pour nous, a suscité, dans un premier temps, le doute chez le CEA-LETI. La discussion s'est donc orientée sur (1) l'état d'avancement de notre contribution à l'état de l'art autour des notions de risque, de confiance et de « Privacy » (2) la présentation de la matrice (3) la spécification de la nature ainsi que de la fonction des scénarios d'usage et notamment leurs différences avec les scénarios d'attaque.

Cette première phase nous a permis de donner à voir certains écueils que nous avons eu à surmonter. Le CEA-LETI a pu mesurer le caractère laborieux mais nécessaire du travail de déconstruction et de reconstruction de l'objet de recherche pour élaborer l'état de l'art. Tant et si bien que nous avons terminé par constater une certaine proximité entre problèmes rencontrés qu'il s'agisse d'objets « sociaux » (« Privacy »/risque/confiance) ou de dispositifs « techniques » (NFC/RFID/CPM) dans leur définition respective. A titre d'exemple, nous

avons exposé au CEA-LETI la difficulté pour nous de construire, lors de cette première phase d'implication de Umanlab dans le projet, une grille standardisée d'évaluation du niveau de risque : les différences entre risques scientifiques et risques perçus, la distribution sociale de la perception des risques, la prise en compte des comportements d'aversion ou d'attraction pour le risque ont été des éléments introduits pour témoigner de la complexité des objets en présence. Enfin, nous avons décidé de livrer, pour le prochain comité de pilotage, les bases définitionnelles sur lesquelles nous nous appuierons pour construire les scénarios d'usage.

Le CEA-LETI ne s'est pas opposé à la matrice présentée, ni dans la forme, ni dans le principe. En effet, en imaginant oralement des ébauches de scénarios d'usage à partir de scénarios d'attaque et insérés dans des domaines d'application divers, nous avons pu, ensemble, constater l'intérêt de notre démarche mais également relever la richesse des combinaisons possibles entre ces trois facteurs<sup>1</sup>. Surtout, il semble qu'un consensus soit né de cette phase en ce qui concerne la nécessité d'un travail collaboratif de construction des scénarios sous la forme d'une journée de travail mêlant acteurs techniques et sociologues (prévue cinq jours avant le prochain comité de pilotage).

Un consensus s'est même dégagé sur le contenu de la matrice : il était impossible dans le temps imparti et avec les moyens accordés d'étudier l'ensemble des configurations d'usage offertes. A cet égard, le CEA-LETI a affirmé privilégier certains types d'attaque (attaques en relais) tout en ignorant les priorités d'Inside en la matière. En tant qu'acteur industriel, il appartenait prioritairement à Inside de fixer les scénarios d'attaque présentant un intérêt pour eux. Ce devait être l'objet d'une réunion téléphonique préalable à la tenue du prochain comité de pilotage.

Enfin, le chef d'équipe de Umanlab a impulsé une discussion importante autour d'un point jusqu'ici négligé : il a rappelé que les problèmes de sécurité auxquels essaient de répondre les ingénieurs (Intégrité, confidentialité, authenticité, disponibilité pour les cryptologues ou accès, identité, contenu, continuité pour ceux travaillant sur la couche physique) trouvaient un écho dans la problématisation à l'œuvre dans les scénarios d'usage.

---

<sup>1</sup> En effet, l'identité entre scénarios d'usage et scénarios d'attaque semblait acquise du côté du CEA-LETI. Cette discussion a permis de rendre évidente pour tous la possibilité d'avènement de différents scénarios d'attaque pour un scénario d'usage déterminé ; d'un éventail de scénarios d'usage différent pour une seule attaque prise en compte, etc. Le même jeu se complexifie lorsque l'on fait basculer les domaines d'application.

Autrement dit, le choix d'un domaine d'application allait conditionner une *configuration d'usage* particulière (acteurs en présence, type d'interaction et enjeu de l'interaction), celle-ci comportant *per se* des dimensions de « Privacy » mises en jeu par l'action. L'un de ces types d'action pouvant être un scénario d'attaque auquel le CPM devrait répondre en matière de sécurité.

Le rôle des scénarios d'usage fixé, nous nous sommes fixés comme objectifs l'écriture de premiers synopsis pour le comité de pilotage. Cette décision a pris acte à l'avance des précisions apportées par Inside quant aux scénarios d'attaque les plus pertinents et aux domaines d'application qui intéressaient le plus nos partenaires.

En interne, nous nous sommes fixés des objectifs propres pour la réunion téléphonique de préparation du comité de pilotage :

- S'assurer de l'implication d'Inside et de la prise de décision de l'ensemble des partenaires quant aux orientations à donner au projet (domaines d'application ; scénarios d'attaque)
- Rendre plus claire l'utilité des scénarios d'usage
- Réaffirmer notre position non leader dans le projet (rapport entre degré d'engagement, moyens alloués et objectifs présents dans l'annexe technique)

#### **h) Conférence téléphonique (T0 + 7)**

Participants : CEA-LETI (1), UVSQ (1), UMANLAB (1 – chargé de recherche)

L'ordre du jour de la conférence téléphonique était le suivant :

- Aspects administratifs
- Définition des scénarios
- Liste des scénarios
- Table des matières de l'état de l'art
- Démarrage du WP2 (conception des différentes fonctionnalités à inclure dans le CPM)

Umanlab a fait part de l'avancée du travail sur les notions de « Privacy », de risque et de confiance. Lorsqu'a été entamée la question des scénarios, une fois de plus, la discussion a porté sur les scénarios d'attaque considérés comme les plus pertinents d'un point de vue technologique, soit l'« attaque en relais », le « eavesdropping » et le « skimming<sup>1</sup> ». Non sans

---

<sup>1</sup> Voir annexe 4, partie 2.



humour, les participants ont relevé la gêne provoquée par l'homonymie entre scénarios d'attaque et scénarios d'usage, le terme scénario étant indifféremment employés pour les deux :

« CEA-LETI – En fait, ça devient difficile parfois de s'y retrouver. (rires)

Umanlab – mais, nous sommes bien d'accord, c'est pas la même chose ?

UVSQ, CEA-LETI – oui, bien entendu...

UVSQ – mais use case et scénario d'usage, c'est synonyme, non ? (rires)

Umanlab – oui, enfin, c'est pas la même langue...

CEA-LETI (chef de projet) – ça c'est sûr, mais bon, faut quand même qu'on parle la même langue pour savoir si on parle de choses différentes (rires). »

Enfin, dans la lignée des discussions sur les scénarios d'attaque, le CEA-LETI (chef de projet) a précisé l'existence de deux types d'attaque : « celles dites *en labo* pour lesquelles la question de la Privacy n'est pas bien cernée et celles dites *dans la rue* qui, semble-t-il, devraient avoir la priorité dans le projet. Il faut qu'on s'accorde dessus lors du prochain copil de septembre. » Des ébauches de critères de sélection des scénarios sont collectivement élaborées<sup>1</sup>.

Le chef de projet a également indiqué qu'il comptait demander à Inside de préciser les scénarios d'attaque et les domaines d'application qu'ils considéraient prioritaires et, à la demande de Umanlab, de confirmer que le téléphone NFC était bien le dispositif à prendre en compte dans le projet comme celui amené à intégrer le CPM.

## ***B - La stabilisation de l'instanciation***

Jusqu'ici, c'était la finalité et l'identité du scénario qui étaient en cours de définition. A partir de cette phase, le scénario s'est mis à glisser vers un objet auquel tous les partenaires devaient apporter leur contribution.

En effet, la frontière entre ce qui relevait du « *technique* » (la sécurité) et ce qui relevait du « *social* » (la « Privacy ») a été floutée à mesure que les interactions entre partenaires se

---

<sup>1</sup> Voir annexe 1, figures 6 et 7.

multipliaient. L'intrigue est devenue de plus en plus solidaire de son environnement de sorte qu'elle s'est mise à former un système dans lequel l'*usage*, la « Privacy », la confiance, le risque et la sécurité étaient des mécanismes encastres. Leurs définitions étaient contingentes de la personne qui les énonçait et l'énonciation de l'un des termes appelait quasi automatiquement celle d'un autre.

Formellement, le scénario a pris corps en stabilisant une partie de la technologie : le téléphone portable et les fonctionnalités NFC. Il comprenait d'abord quatre séquences reprenant les quatre « use cases » exposés par Inside et prenait pour cadre le domaine d'application du transport. Ces séquences ont ensuite été requalifiées comme quatre scénarios à part entière en raison des intrigues distinctes qu'elles comportaient.

Ce premier redécoupage a marqué le début de l'intégration croissante d'éléments de nature hétéroclite dans les scénarios. La description des composantes « techniques » du scénario a gagné en précision tandis que sur le plan de l'environnement, on a assisté à une montée en généralités de plus en plus abstraites. L'environnement du premier scénario (« Payment ») s'est trouvé peuplé d'entités aux contours flous, réduites à des dénominations impersonnelles : Julie aurait tout autant pu s'appeler Juanita ou Jean sans que cela ne bouleverse l'intrigue... Les scénarios sont alors articulés autour d'une séquence narrative à partir desquels des séquences d'action entre utilisateurs et dispositifs techniques étaient déductibles. Chacune de ces séquences a aussi permis de déduire des menaces potentielles.

Ce premier scénario a scellé l'identité des scénarios comme *instanciation de situations d'utilisation* du NFC. Ces situations, cadres contraignants ou habilitants d'attaques, ne mettaient pas en scène le CPM. En effet, le CPM n'était pas situé au centre de l'intrigue, il en était la résolution, et aucun des partenaires n'était encore prêt à définir précisément l'étendue de son rôle. La construction du scénario « Payment » a également fait l'objet d'allers-retours entre différents partenaires.

#### **a) Réunion interne – lancement de l'écriture du scénario (T0 + 8)**

Avant d'entamer l'écriture proprement dite des scénarios, nous avons récapitulé les éléments structurants. Nous avons choisi d'entrer par les domaines d'application et de définir

des configurations d'usage en les croisant avec les attaques potentielles. Nos acteurs étaient des usagers de téléphone NFC dont les enjeux étaient inspirés par les critères CAUTIC<sup>®</sup>, auxquels était rompu le responsable projet (utilisabilité, utilité, identité, environnement social). Ces critères faisaient écho à la manière dont les partenaires « techniques » identifiaient les usagers (« Alice », « Bob » et « Charlie ») avec pour enjeux l'authenticité, la confidentialité, l'intégrité et la disponibilité et l'accès, l'identité, les contenus et la continuité de service pour la partie couche physique<sup>1</sup>. A ce moment, nous ignorions encore le rôle exact du CPM et nous contentions de construire des situations d'usage du NFC vraisemblables qui intégraient des scénarios d'attaque hypothétiques. Lors de nos brainstormings, nous évoquions pêle-mêle des scènes de la vie quotidienne, les scénarios d'attaque, des passages de films, la théorie structurale de Greimas, des souvenirs personnels, les contraintes techniques ainsi que des exemples empruntés à la littérature.

Nous avons choisi, presque par hasard, comme domaine d'application le transport. Notre ébauche de scénario s'est appuyée sur la description sommaire de personnages engagés dans quatre types d'action correspondant aux quatre modalités d'utilisation du NFC<sup>2</sup>. Nous n'avons imaginé qu'un seul type d'attaque pour les quatre cas d'utilisations et en avons ensuite déduits les dommages que cela pouvait causer pour chacun des acteurs à l'aune des critères établis par le CEA-LETI (accès, identité, contenu, continuité de service). Nous avons laissé en suspens les critères que nous avons choisis pour analyser l'usage.

### **b) Comité de pilotage 3 (T0 + 8)**

Présents : CEA-LETI (3), UVSQ (1), Inside (1 + thésarde), UMANLAB (3)

Le début de journée était consacré à un point sur les aspects administratifs et à la finalisation de la table des matières de l'état de l'art. Le compte-rendu de réunion, rédigé par le CEA-LETI, mentionnait : « l'UVSQ a fait une présentation sur les aspects protection de la vie privée et comment ces derniers sont pris en compte et formalisés au niveau protocolaire. Umanlab a fait une présentation de la méthodologie de structuration des scénarios avec comme objectif de les tester sur une population réduite [en fin de projet]. » Le

---

<sup>1</sup> Voir annexe 1, figure 8.

<sup>2</sup> Voir annexe 1, figures 9 à 11.

jeu de transparents ayant servi aux présentations a été diffusé à tous par courrier électronique. L'après-midi, Inside a présenté la technologie NFC et ses différents modes d'utilisation<sup>1</sup> (« use cases »). Enfin, l'ensemble des membres a validé la méthodologie de rédaction et de sélection des scénarios après la présentation de l'ébauche de scénario de Umanlab. Umanlab a évoqué le code PIN comme moyen de sécurisation et Inside a répliqué « qu'il faut différencier le NFC sécurisé avec une autorisation préalable à l'échange de données et le non sécurisé, sans autorisation préalable. »

Dans sa présentation sur l'état de l'art des attaques protocolaires et des modèles de sécurité, l'UVSQ a défini en quoi consistait une analyse de la sécurité (« For each considered protocol, give cryptographic security arguments telling which security requirements are fulfilled by using a security proof and which are not by showing an attack »). Ainsi la notion de sécurité reflétait une menace qui impliquait d'identifier les buts de l'attaquant et un modèle de déroulement de l'attaque<sup>2</sup>. Ainsi, la preuve de sécurité se démontrait de deux manières : soit en essayant de monter une attaque (si l'attaque réussit, le système n'est pas sûr ; si elle échoue, rien ne peut être affirmé), soit en prouvant qu'aucune attaque n'est réalisable sous certaines conditions. En réponse à une question de Umanlab, l'UVSQ a affirmé que la séparation entre la couche physique et la couche protocolaire était analytique mais « qu'en réalité, les deux sont mêlées. »

La présentation d'Inside est centrée sur l'intégration du NFC dans le téléphone portable. Technologiquement, les solutions d'intégration sont multiples, ce qui expliquait en partie l'absence de modèle économique stabilisé. Inside a également relevé que le déploiement géographique de la technologie se faisait essentiellement en Asie et en Europe. Enfin, l'industriel a présenté les produits qu'il offrait et souligné que sa puce Microread® était la préférée de la GSMA<sup>3</sup>. L'un des membres de Umanlab a demandé si le SPAM ou les virus informatiques rentraient dans le cadre de l'étude tandis qu'un autre a embrayé sur l'internet mobile.

---

<sup>1</sup> Voir annexe 1, figures 12 et 13.

<sup>2</sup> Voir annexe 1, figures 17 et 18.

<sup>3</sup> GSM Association, association mondiale qui représente 850 opérateurs de téléphonie mobile. Voir chapitre 4.

A ce moment, le scénario transport comprenait quatre séquences reprenant les quatre modes d'utilisation (« use cases »).

### **c) Conférence téléphonique (T0 + 9)**

Présents : CEA-LETI (2 ), UVSQ (1), Inside (1), UMANLAB (3)

Pour la conférence téléphonique, nous (Umanlab) avons choisi de nous concentrer sur la première séquence du scénario, dite « Payment » afin de fournir une description de l'attaque plus complète. C'est la première fois que nous faisons intervenir le CPM, que nous nommions souvent COPRIM par facilité de langage. Les scénarios étaient donc enrichis et l'intrigue était découpée en séquences (prologue, attaque réussie, attaque échouée) et par personnages (Alice, Charlie 1 et 2). La présence de deux Charlie s'expliquait par les nécessités de l'attaque en relais. C'est cette version qui a été envoyée aux partenaires<sup>1</sup>.

Par souci de clarification des échanges, le scénario a été scindé en plusieurs parties. Les partenaires se sont accordés pour que chaque « use case » qui rythmait la narration soit considéré comme un scénario à part entière. En effet, la vérification de la faisabilité et de la plausibilité de ces nouveaux scénarios demandaient aux partenaires techniques un travail différencié.

C'est à Inside et l'UVSQ qu'a échue la mission de préciser les protocoles utilisés ainsi que les attaques potentielles pour chaque scénario. Ensuite, le CEA-LETI devait se joindre à eux pour détailler les chemins d'attaque possibles. En amont, Umanlab et le CEA-LETI devaient prolonger leurs efforts de travail en commun pour la rédaction des trois scénarios restants, les développements présentés par Umanlab méritant d'être corrigés.

En fin de réunion, des discussions se sont engagées au sujet du scénario « Payment ». Il s'agissait de s'accorder sur la durée effective des transactions électroniques (en millisecondes et à une dizaine de centimètres). Nous nous sommes également mis d'accord sur la possibilité d'implémenter un code PIN.

---

<sup>1</sup> Voir annexe 1, figures 14 à 16.

#### **d) Réunion interne (T0 + 10)**

L'échéance de la livraison des premiers livrables à l'ANR approchait et la rédaction de l'état de l'art prenait de plus en plus le pas sur les réflexions sur les scénarios. Néanmoins, il nous paraissait important de ne pas perdre de vue le fait que l'état de l'art devait nourrir l'écriture des scénarios. Nous souhaitons également organiser une nouvelle rencontre avec le CEA-LETI afin d'avancer sur la rédaction des trois scénarios restants.

#### **e) Réunion téléphonique (T0 + 10)**

Présents : CEA-LETI (2), UVSQ (1), Inside (1 - doctorante), UMANLAB (2)

Le début de la réunion a été marqué par l'intervention d'Inside, représentée par une doctorante dont la présence était alors limitée à une participation à un comité de pilotage. Elle a soulevé le fait que la question de la « Privacy » était presque absente des scénarios. Sa remarque a été appuyée par le chef de projet, qui a insisté sur l'impératif d'« avoir dans les scénarios un lien entre le sans contact et la Privacy qui sont l'essence du projet ». Ces remarques passées, le déroulement de la réunion a respecté l'ordre du jour prévu, soit la définition des aspects protocolaires des scénarios ainsi que quelques points administratifs.

Inside et l'UVSQ ont travaillé sur l'aspect protocolaire des scénarios. Dans une première phase, l'objectif était de préciser les scénarios présentés à la réunion précédente afin d'obtenir une description satisfaisante pour la suite du projet. Dans une deuxième phase, cela permettait au CEA-LETI, à Inside et à l'UVSQ d'analyser les attaques potentielles. La troisième phase était consacrée à la proposition de contre-mesures.

Points abordés et remarques :

Certains protocoles étaient confidentiels. Le travail d'Inside et de l'UVSQ a consisté à en extraire les points pertinents pour le projet afin de pouvoir travailler sur des modèles génériques et significatifs de protocole. Ils ont évoqué la possibilité de prendre en compte virus ou chevaux de Troie transmis par le réseau cellulaire sur téléphone mobile et utilisant le lien sans contact

La fin de réunion est à nouveau marquée par un rappel à l'ordre du CEA-LETI par rapport aux objectifs du projet : « introduire dans le scénario des aspects très liés aux données

personnelles, comme la fuite de données figurant dans des agendas, des photos, des emails, des choses comme ça ! »

En réaction, Umanlab a proposé pour la rencontre suivante une présentation structurée des aspects concernant la protection de la vie privée incluant à la fois des données personnelles ainsi que les actions réalisées par un individu relevant du domaine privé et pouvant être observables, à travers le sans contact.

### ***C - L'émergence de champs du possible***

Les différents cas possibles sont cette fois-ci accompagnés des réponses possibles du CPM. Les scénarios sont devenus un outil d'évaluation et de description.

Le volet descriptif, après avoir fait l'objet d'une traduction des séquences narratives en procédures techniques, est complété par une autre opération de traduction : cette fois-ci, par l'intermédiaire de Umanlab, les procédures techniques sont traduites en séquences d'usage. Cette dernière étape de scénarisation est caractérisée par l'intensité des échanges entre partenaires et notamment entre Umanlab et Inside.

C'est dans l'évaluation des menaces et des solutions apportées que la notion de « Privacy », déclinée à l'aide d'une utilisation opérationnelle de trois variables (« risque », « contrôle », « feedback »), est la plus mobilisée. En somme, tandis que le concept devait servir de ressource primordiale à l'élaboration des scénarios, il a supporté plusieurs opérations de traduction avant de recouvrer un rôle prépondérant durant l'élaboration de la partie évaluative des scénarios.

Ce faisant, la « Privacy » a été transformée en concept commensurable traduisant le détachement progressif des scénarios d'une logique de l'usage à une logique d'utilisabilité. Ainsi, la stabilisation de la description de la technologie a déclenché une réapparition des figures de l'utilisateur en contact direct avec le dispositif : opérateurs, industriels, contrôleurs de billets, sociétés de mobilier public.

Cependant, bien que les scénarios aient réussi à fournir une instanciation du fonctionnement du NFC, un inventaire des possibilités d'action du NFC et une grille d'évaluation des enjeux soulevés en termes de « Privacy », l'équipe-projet considérait le

travail d'évaluation comme étant encore à l'état de balbutiements. Les contributions de Umanlab, lorsqu'elles n'ont pas déçues en ce qu'elles ne constituaient pas un « go/no go », ont été considérées comme un tremplin pour l'élaboration d'une évaluation technoscientifique des propositions. Le document final a eu pour titre définitif « analyse des scénarios » en lieu et place de « spécifications du CPM. »

#### **a) Comité de pilotage 4 (T0 + 11)**

Présents : CEA-LETI (3), UVSQ (2 dont la doctorante), Inside (2 dont une doctorante), UMANLAB (3)

A l'ordre du jour étaient inscrits la validation du plan des états de l'art, un point sur la description des scénarios et un point administratif.

L'ensemble des partenaires se sont accordés sur la forme du document comprenant les scénarios. Ce document, nommé « spécifications CPM » est organisé en trois parties<sup>1</sup>. Une première partie devait être consacrée à la description générale des scénarios. La seconde partie à un gros plan sur chacun des scénarios avec le détail des protocoles à l'œuvre, des attaques possibles et une analyse de risque pour évaluer la pertinence et la priorité des attaques à traiter dans le cadre du projet. Les spécifications techniques préliminaires (protocole applicatif pour Inside et UVSQ, protocole de communication pour CEA-LETI, attaques sur le sans contact pour Inside, UVSQ et CEA-LETI à traiter et enfin analyse de risque et priorité des attaques par tous) constituaient la troisième partie du document.

La doctorante de l'UVSQ, nouvelle venue dans le projet, a exprimé sa surprise devant le scénario déjà produit (« Payment »). Elle considérait qu'il ne soulignait pas suffisamment la menace de la « Privacy ». Une vive discussion s'en est suivie entre Umanlab et la doctorante de l'UVSQ sur ce que recouvrait la notion de « Privacy ». Les membres de l'équipe Umanlab se défendaient en arguant du fait que la notion de « Privacy » comprenait de nombreuses acceptions et que les résultats de leur travail sur l'état de l'art du concept permettaient de comprendre ce premier scénario comme une illustration de la mise en jeu du concept. La doctorante de l'UVSQ a souligné le fait que la question n'était vraiment approfondie que sous l'angle « technique » et qu'elle ne voyait pas dans les exemples des situations vraisemblables « dans la vraie vie ». Le chef de projet (CEA-LETI) a clôturé l'échange

---

<sup>1</sup> Voir annexe 4.



en affirmant, habilement, que le scénario « peer to peer » était certainement celui qui mettait le plus en jeu la « Privacy » de l'utilisateur puisque c'était le seul dans lequel « deux vrais utilisateurs échangent des données. »

Les partenaires se sont ensuite entendus sur un planning de travail. Un premier document intermédiaire est prévu. Il devait contenir une présentation des quatre scénarios par Umanlab assortie d'une étude de la dimension « Privacy » pour ceux-ci pour la fin du mois de février. En parallèle, Inside et l'UVSQ devaient procéder à l'analyse du scénario « Payment », l'objectif étant de livrer pour T0 + 14 une analyse complète de l'ensemble des scénarios.

La réunion s'est achevée sur l'annonce de départ de la doctorante d'Inside en T0 + 12 et dont le remplaçant serait encore un doctorant avec lequel nous fîmes connaissance par mail quelques jours plus tard.

Jusqu'au prochain comité de pilotage prévu pour en T0 + 13, l'essentiel du travail des partenaires est tourné vers la livraison des états de l'art T0 + 12. Le travail sur les scénarios est alors mis en jachère.

#### **b) Réunion interne (T0 + 13)**

L'analyse complémentaire produite par Inside et UVSQ sur le scénario « Payment » nous est parvenue quelques jours avant le comité de pilotage. Nous avons été surpris par le niveau de détail ajouté à notre première version sur le plan narratif : l'histoire était désormais jalonnée de précisions techniques. Nous notions que le scénario était décliné en plusieurs « use cases ». Trois possibilités techniques étaient présentées pour l'usage du NFC. Il nous semblait que certaines de ces possibilités pouvaient influencer sur le déroulement du scénario. Nous avons décidé de confirmer notre compréhension du document lors du comité de pilotage. Enfin, nous réfléchissions au moyen de valoriser, sur la scène académique, les travaux entrepris jusqu'ici.

#### **c) Comité de pilotage 5 (T0 + 13)**

Présents : CEA-LETI (2), UVSQ (1 + doctorante), Inside (1 + nouveau doctorant), UMANLAB (2 – responsable projet excusé)

Ce comité de pilotage était consacré à l'état d'avancement de chacun des partenaires, incluant notamment un point sur la rédaction des scénarios et la consolidation de leur contenu. Les discussions portant sur les spécifications du CPM devaient clore la réunion.

Le CEA-LETI a présenté un état d'avancement du travail effectué concernant les attaques tandis qu'Inside a présenté le document rédigé avec l'aide de l'UVSQ sur les scénarios. Une discussion s'est engagée sur ce premier scénario (« Payment ») et particulièrement autour des particularités propres à chaque option technologique présentée. Inside a précisé que la première option était peu réaliste en raison de la clé cryptographique utilisée : « les clés statiques permanentes ont peu de chances d'être implémentées, ici. » Pour le deuxième cas, une argumentation technique a également été développée en différenciant deux facteurs de génération de clés cryptologiques. Le responsable projet Inside a précisé que l'une était privilégiée par les Etats-Unis tandis que l'autre avait les faveurs de l'Europe. Concernant la troisième option technologique (le code PIN), Inside a affirmé que « cela n'est pas fait sur le NFC mais c'est assez probable, logique, que les solutions y ressembleront. » Le responsable projet Inside notait qu'au niveau des transactions bancaires, « les institutions financières disposent de systèmes de cotation des attaques avancées. » Il a terminé en affirmant : « de toute façon, dans le NFC aujourd'hui, il y a beaucoup de flottement... c'est une technologie non stabilisée. Des expérimentations sont en cours mais il y a beaucoup d'incertitude autour de la certification. »

Il est décidé qu'Inside et l'UVSQ devaient approfondir leur analyse du scénario « Payment » pour T0 + 14. Les critères de sélection des options techniques pertinentes seraient ensuite utilisés pour évaluer les trois autres scénarios qu'il restait à compléter soit les scénarios « transport », « smart poster » et « peer to peer ». Une table des matières du document a été validée tandis que le chef de projet a rappelé que les scénarios allaient servir d'introduction au document de spécifications du CPM. Enfin, concernant les volontés de valorisation exprimées par Umanlab, Inside a demandé que soit instauré un accord préalable du consortium avant publication.

#### **d) Réunions internes (T0 +15<sup>1</sup>)**

Durant plusieurs réunions, nous avons discuté de la manière d'évaluer les menaces qui pesaient sur la « Privacy » du CPM, dont le fonctionnement nous échappait encore dans sa globalité. Par ailleurs, les conclusions que nous avons tirées dans l'état de l'art nous compliquaient la tâche : la notion de « Privacy » nous apparaissait de plus en plus comme une notion complexe, protéiforme et fortement dépendante des contextes d'utilisation et de la perception de l'utilisateur. Cependant, ce travail nous a permis de découvrir plusieurs pans de littérature spécialisée dans l'électronique et les interactions homme-machine (HCI), littératures caractérisées par une volonté d'opérationnalisation des recherches. Ainsi, pour apporter notre pierre à l'évaluation des scénarios, nous avons intégré une grille d'analyse empruntée au HCI qui permettait, *a minima*, de rendre l'utilisateur potentiel présent durant la conception. Les deux variables clés constituant cette grille étaient celles du « contrôle » et du « feedback » offerts à l'utilisateur et nous permettaient de visualiser sur un même plan les différences entre options techniques en termes d'implication de l'utilisateur dans l'usage du CPM. Ainsi, les trois options techniques figurant dans le scénario « Payment » élaboré par Inside et UVSQ ont été intégrées dans la démarche d'évaluation après que nous nous soyons acharnés à les comprendre, sans être pour autant certain d'y être parvenus. Ce faisant, en prenant en compte la manière dont ces options pourraient être perçues par l'utilisateur, nous avons découpé l'une d'elles en deux possibilités d'usage. Au total, nous obtenions donc quatre « options d'usage » pour trois « options techniques<sup>2</sup> ».

En deuxième lieu, nous avons choisi d'élaborer des hypothèses à partir de cette première analyse en nous basant sur le travail effectué durant la revue de littérature sur la notion de confiance. Il s'agissait pour nous de comprendre sur quelle entité l'utilisateur devait se reposer et conséquemment vers qui il pourrait se retourner en cas d'échec de la protection.

Enfin, nous avons élaboré une dernière partie plus spéculative destinée à servir de base d'écriture à la version des scénarios qui devaient servir aux tests auprès des utilisateurs potentiels en fin de projet. Cette dernière partie a également marqué l'aboutissement d'une réflexion sur l'usage différencié des scénarios et sur les formes qu'ils devaient prendre en conséquence.

Ce document en trois parties est envoyé à l'ensemble de consortium en préparation de la réunion téléphonique du 4 mai.

#### **e) Conférence téléphonique (T0 + 15)**

Présents : CEA-LETI (2 ), UVSQ (2 dont la doctorante), Inside (1- nouveau doctorant), UMANLAB (2 – responsable projet excusé)

---

<sup>1</sup> Il nous faut préciser qu'à partir de ce moment, les absences du responsable projet Umanlab se sont faites de plus en plus espacées.

<sup>2</sup> Voir annexe 3.

Le doctorant d'Inside et moi-même avons présenté le document « Payment » consolidé. Les premières remarques ont porté sur le mode de fonctionnement du lien sans contact et des imprécisions liées dans le document. Le CEA-LETI a demandé à ce que le mode de fonctionnement soit précisé « car s'il est en ISO 14443 ou ISO 15693 ou Peer to Peer actif, les menaces et vulnérabilités sont pas du tout les mêmes ! ». Par ailleurs, nos interlocuteurs ont apprécié d'avoir vu apparaître le terme confiance dans l'analyse « sociologique » mais notent deux facteurs importants à prendre en compte : la sécurité du point de vue des opérateurs et le possible surcoût industriel des solutions proposées. Très rapidement, après discussion, le chef de projet a précisé que le consortium ne pourrait apporter de recommandations que sur les premier et dernier points, au vu de l'absence d'opérateur téléphonique dans le projet.

Les scénarios restant à traiter sont alors considérés comme plus complexes par les partenaires techniques. Les scénarios « transport » et « smart poster » demandaient à inventer des procédures inédites concernant respectivement les contrôles de billet et ceux de l'authenticité des tags déposés dans les posters. Ce caractère innovant a poussé le chef de projet à inciter les partenaires à des échanges plus intenses. Le dernier scénario, « peer to peer » suscitait encore de grandes attentes en termes de mise en jeu de la « Privacy. »

Tandis que le premier scénario a été rédigé en français, le chef de projet a rappelé que puisque les scénarios devaient faire partie d'un livrable, il importait de les traduire en anglais, langue sur laquelle nous nous étions accordés pour communiquer avec l'ANR.

#### **f) Réunions internes et échanges avec Inside/UVSQ (T0 + 15-17)**

Le responsable projet ne participait plus que sporadiquement aux réunions internes mais il veillait à la validation des rendus finaux. Cette fois-ci nous échangeons avec Inside et l'UVSQ sur des points techniques qui nous paraissaient importants en termes d'usage. Le dialogue était constant, notamment avec le doctorant d'Inside qui s'intéressait particulièrement à la notion de « Privacy » et nous relançait régulièrement sur des aspects de l'état de l'art qui ne lui avaient pas semblé clairs. Nous remarquons que des indications portant sur l'usage (scénario « peer to peer ») étaient présentes dans la description technique.

#### **g) Comité de pilotage 6 (T0 + 17)**

Présents : CEA-LETI (2), UVSQ (1 – la doctorante a quitté l'établissement), Inside (3 dont le doctorant), UMANLAB (2 – responsable projet excusé)

Ce comité de pilotage se tenant à Aix-en-Provence, siège d'Inside, nous nous sommes rendus en voiture sur les lieux avec les partenaires du CEA-LETI. Durant le trajet, l'un des membres du CEA-LETI, parcourant le document fourni par Inside et UVSQ, s'est tourné vers

nous et nous a demandé une précision technique sur l'un des cas décrits. Une discussion d'un quart d'heure s'est alors engagée sur la lecture et la compréhension des autres cas entre membres du CEA-LETI et Umanlab (à noter l'absence du responsable projet).

Après passage en revue des points administratifs, cette réunion s'est ouverte par une présentation de prototypes NFC disponibles chez Inside. L'essentiel de la journée était destiné à la finalisation des travaux sur la construction des scénarios.

La première décision prise par le comité de pilotage a été de substituer le nom du document « analyse des scénarios » au livrable « spécifications du CPM » en raison du retard pris dans le projet. Le chef de projet argue que « le document « analyse des scénarios » représentait déjà un très bel effort de clarification des situations typiques liant le NFC à la vie privée, et de les analyser selon la perspective sociétale. » (Compte-rendu du comité de pilotage, chef de projet).

A suivi la présentation de cas d'application par un « responsable de ligne produit » d'Inside. Nous ont été présentées des applications proches des scénarios « smart poster » et « Payment » sous formes de prototypes. Un échange de questions s'en est suivi sur les développements contemporains du NFC en termes d'usage. Notre interlocuteur nous a précisé que le NFC Forum ne travaillait pas en mode actif/actif pour le « peer to peer », que pour les échanges de fichiers entre deux téléphones NFC, un couplage des technologies NFC et Bluetooth était en vigueur et que c'était en Allemagne que l'usage du NFC dans le domaine du transport présentait le plus de promesses.

Ces précisions nous ont engagés sur une discussion de fond concernant le contenu des scénarios et des analyses. Après le scénario « Payment », traité lors du dernier comité de pilotage, Inside a présenté les trois autres scénarios NFC restant : le « transport », le « smart poster » et le « peer to peer ». Pour chaque scénario, plusieurs options techniques ont été présentées. Une analyse des menaces a été faite pour chaque option technique. Le consortium a remarqué que les scénarios « Payment » et « transport » semblaient plus étoffés que les deux autres.

Umanlab a ensuite présenté le travail effectué sur le reste des scénarios. De la grille développée par Umanlab, deux éléments ont retenu l'attention du CEA-LETI : « Le quadrant en haut à droite avec beaucoup de « feedback » et peu de « contrôle ». L'utilisateur gère complètement le dispositif par rapport à sa vie privée. Mais c'est potentiellement lourd. Et, le

quadrant en bas à gauche. La sécurité est implicite et l'utilisateur fait confiance dans le système et ses fonctions de protection de la vie privée<sup>1</sup>. »

Néanmoins, un des interlocuteurs du CEA-LETI nous a apostrophé par une question inattendue : « malgré la qualité du travail, vous n'auriez pas une méthode pour nous dire clairement ce qui va vraiment inquiéter les utilisateurs ? Par exemple, nous dire pour chacun des scénarios quel serait la meilleure option technique d'un point de vue de l'acceptation sociétale ? »

Personnellement échaudés, nous avons répondu que si nous détenions ce type d'informations nous serions déjà riches. De manière surprenante, c'est le doctorant d'Inside qui a coupé court à l'échange en affirmant que « même d'un point de vue strictement technique, il nous est difficile de vraiment décider ce sur quoi nous devons travailler en priorité. » L'intervention du doctorant a ouvert une période de discussion intense essentiellement animée par lui et moi. A partir des plans d'évaluation (« contrôle/feedback »), nous discutons la position des points (« options techniques ») en fonction des explications complémentaires qu'il fournissait pour faciliter la lecture du document. La grille permettait de mettre en lumière notre mauvaise interprétation de certains protocoles techniques quand elle ne soulignait pas l'appropriation de certaines attitudes « sociétales » par Inside. Ainsi, plusieurs dénominations données aux « options techniques » sur les plans « contrôle/feedback » sont portées à discussion. Au départ, nous avons modifié les appellations originales pour des raisons purement esthétiques, les noms de plusieurs options étant trop longs. Cependant, lors de la discussion, nous avons conservé les dénominations courtes, de même que nous utilisons les notions de « trust » et « confidence » sans avoir à rappeler leurs définitions. Aussi, la notion de *configuration d'usage*, renvoyant à un quadrant du plan, était complètement assimilée par le doctorant d'Inside ainsi que par le cryptologue de l'UVSQ. Les autres partenaires lui préféraient encore le mot quadrant. Par ailleurs, plutôt que de parler de mode actif ou passif pour le NFC, j'avais adopté le langage du doctorant d'Inside en parlant de mode « écoute » et de mode « initiateur », autre terminologie recouvrant les mêmes fonctions. Le doctorant a également à plusieurs reprises questionné les notions de « feedback » et de « contrôle », puis les a utilisées pour discuter l'exactitude de la position des points. Concernant l'usage de la notion de « Privacy », j'ai signalé qu'elle était souvent

---

<sup>1</sup> Voir annexe 3, partie 2.1.

utilisée en lieu et place du mot sécurité dans les parties techniques. Le chef de projet m'a répondu que cela ne nuisait pas à l'essentiel puisque « les parties sociétales permettent de mieux comprendre les autres dimensions de la notion. » Enfin, j'ai soulevé une question qui représentait une inconnue pour moi : « est-ce que l'on doit considérer dans l'ensemble des scénarios que le téléphone mobile est doté d'une fonction d'activation et de désactivation des échanges sans contact ? » Une fois de plus, le doctorant d'Inside m'a répondu en premier : « c'est vrai que c'est l'inconnue orthogonale à l'ensemble des cas que l'on a traité. La question que tu poses en fait, c'est : est-ce que le rôle du CPM est de sécuriser juste la carte que contient le téléphone ou doit-il jouer le rôle de brouilleur ? » Le CEA-LETI, reprenant au vol l'idée de brouilleur, a affirmé que la question était cruciale pour le projet et qu'elle restait à traiter.

#### **h) T0 + 17-19**

Plusieurs échanges de mails ont lieu entre Inside et Umanlab pour finaliser l'ultime version du document « analyse des scénarios ». Celui-ci est finalement organisé ainsi :

- Une introduction présentant la méthode d'analyse rédigée par Umanlab
- La présentation générale des scénarios sous forme exclusivement narrative, rédigée par Umanlab
- Une partie rappelant l'aspect polymorphe de la notion de Privacy, rédigée par Umanlab
- Une partie comprenant une description technique détaillée de chaque scénario (options techniques, menaces relatives et solutions proposées) suivie d'une analyse sociétale (« control »/ « feedback » ; « trust »/ « Privacy »), rédigée par Inside/UVSQ et Umanlab
- Une conclusion, rédigée par Umanlab<sup>1</sup>

#### **i) Conférence téléphonique (T0 + 20)**

Présents : CEA-LETI (2), UVSQ (1), Inside (2 dont doctorant), UMANLAB (3 – dont responsable)

---

<sup>1</sup> Voir annexe 3, sommaire.

Préalablement à la conférence téléphonique, nous avons tenu une ultime réunion en interne pour définir les points que nous souhaitions aborder. Nous nous interrogeons sur la nature du document « analyse des scénarios ». Nous pensions alors que ce document ne répondait que partiellement à ce que nous envisagions au départ du projet. En effet, nous avions le sentiment que bien que les scénarios écrits aient permis de contextualiser des menaces potentielles et des contre-mesures adaptées, nous doutions que l'objectif de classement initial ait été atteint. Par ailleurs, la question de l'intégration du CPM au téléphone n'avait toujours pas été résolue. C'est donc non sans une certaine appréhension que nous abordions la conférence téléphonique.

Trois points devaient être abordés : la validation du livrable « Analyse des scénarios », l'organisation des travaux sur spécifications du CPM ainsi qu'un point sur la préparation de la revue de projet ayant lieu en T0 + 20.

La réunion s'est ouverte par un long échange entre le CEA-LETI, Inside et l'UVSQ, les premiers étant demandeurs de clarifications sur des points portant sur les questions protocolaires. Suite à cet échange d'environ trois quart d'heures, le chef de projet a poursuivi en affirmant que « les scénarios traitent des menaces et contremesures mais pas du rôle du CPM qui reste à spécifier. C'est le travail que nous devons entamer avec le document spécifications du CPM. » Il est également convenu que ce travail ait permis d'obtenir un aperçu de ce que serait un « CPM idéal » mais qu'il fallait désormais, pour obtenir des spécifications plus détaillées, être capable d'établir des priorités relatives à l'importance des menaces et à la mise en œuvre des contremesures. L'autre interlocuteur du CEA-LETI a poursuivi en affirmant qu'une analyse de vulnérabilité du lien sans contact a donc été établie, que nous avions connaissance des principales attaques liées et que pour faire ce travail de spécification du CPM, « il faudrait essentiellement s'appuyer sur l'annexe technique du projet. »

Relativement à cette dernière remarque, je me suis légèrement emporté et ai apostrophé les interlocuteurs en leur demandant la raison d'être du travail d'élaboration des scénarios, des analyses « sociétales », de la volonté de réfléchir au rôle de l'utilisateur et à la notion de « Privacy » : « à quoi sert tout ce qu'on a fait au final, parce que je comprends plus vraiment... quel est le but des scénarios et surtout à quoi ils vous ont servi au fond ? » Le chef de projet répond immédiatement : « sans les scénarios, le travail que nous allons entamer



n'aurait pas été possible. Sans scénario, on n'aurait pas d'idées pour le démonstrateur, ni peut-être d'idée des utilisateurs. Maintenant, il nous reste à décider quelles sont les menaces prioritaires et en fonction de cette décision on va pouvoir savoir dans quelle direction aller pour les spécifications puis pour le démonstrateur du CPM. » Le cryptologue d'UVSQ a ajouté que les scénarios ont permis de « parler sur du concret avec des situations vraies ». Le chef de projet a conclu que « l'objectif ultime est d'intégrer le CPM dans les scénarios et que ça servira peut-être pour les études d'usage de troisième année. »

La réunion s'est conclue par la fixation d'un rendez-vous en T0 + 20 pour préparer la revue de projet devant l'ANR. Le document « analyse des scénarios » est envoyé le soir même comme livrable. Lorsque nous avons raccroché, notre responsable de projet nous a demandé si nous avions « capté quelque chose aux discussions techniques et aux différentes sortes de menaces et spécifications ? » J'ai répondu par l'affirmative : « la plupart des éléments, oui, mais sur les "spec" je suis un peu énervé parce que du coup le lien entre scénarios et "spec", on va pas le voir ! »

**Fin de l'observation participante.**

## RÉSUMÉ

L'« hypercompétitivité » (D'Avenir & Gunther, 1994) qui caractérise notre environnement économique contemporain fait de l'innovation une préoccupation stratégique pour les organisations. Celles-ci tentent de répondre à cette injonction par le recours à une multitude de « systèmes experts », caractéristique de la « modernité avancée » (Giddens, 1990). Parmi ceux-ci, la stimulation des activités de R&D est reconnue comme une contribution majeure qui nécessite l'utilisation croissante de champs d'expertises variés. C'est dans ce contexte que les sciences sociales sont mobilisées comme forme d'expertise contributives des « recherches spéculatives pour l'innovation » (Stewart & Claeys, 2009). Ces recherches interviennent en amont de processus d'innovation, en un lieu nommé « Fuzzy Front End » (Smith & Reinertsen, 1995), lieu dans lequel se forge la construction de la réalité sociale de l'invention : son usage ou plutôt sa projection. Notre thèse s'interroge sur ces technologies de production de connaissances que sont les projections d'usage et ambitionne de rendre intelligibles les politiques qu'elles mettent en oeuvre, la performance des collectifs mobilisés sur les recherches et sur eux-mêmes ainsi que les arrangements déployés par les acteurs durant ces processus. Notre immersion dans le tissu industriel grenoblois, et en particulier dans l'environnement du CEA-LETI, nous a permis de proposer une lecture des projections d'usage comme des compositions de fictions axiomatiques au service de la recherche technologique. En scrutant le concept d'usage, nous mettons en lumière les carrières empruntées par celui-ci et les mutations des pratiques associées. En interrogeant l'une des formes de la projection d'usage, le scénario, nous mettons en évidence les liens entre performativité et recours à la fiction. En interrogeant les mutations des composantes du projet, nous démontrons le caractère axiomatique des projections, en tant que forme de réponse à une demande sociale qui émane de plusieurs endroits et dont l'exigence de production de savoirs actionnables nécessite de composer avec des données en mouvement.

## SUM UP

Innovation is today a major and strategic asset for organizations that compete in a hypercompetitive world (D'Avenir & Gunther, 1994). They are trying to face these new challenges, by using a diversity of “expert systems” typical of our « advanced modernity » (Giddens, 1990). Amongst those, boosting R&D activities is major inputs that demand the use of different expertises. Speculative researches for innovation are one of them. They take place in the “Fuzzy Front End” of innovation, a place where the construction of the social reality of invention is made : its usage, or to be more precise, its projection. Our thesis examines these knowledge-producing technologies and tries to make understandable the policies at work, the performance of embedded collectives on the innovation itself, and on themselves, and the arrangements made during this process. Our work in the Grenoble industrial area and collaboration with the CEA-LETI helped us to propose an understanding of these projections as compositions of axiomatic fictions for technological research. Analyzing the concept of usage, we highlight its careers and the mutation of associated practices. Interrogating one form of projection, the scenario, we show the links that lie between fiction and performativity. By leaning on the project mutating components, we demonstrate the axiomatic character of the projection, understood as a form of answer made to a social demand that comes from different places, and whose necessity of actionable knowledge is solved by composing with moving data.